

IN THE INVESTIGATORY POWERS TRIBUNAL

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Defendants

[draft] RE-AMENDED STATEMENT OF GROUNDS

INTRODUCTION

1. Privacy International is a leading UK charity working on the right to privacy at an international level. It focuses, in particular, on challenging unlawful acts of surveillance.
2. The Secretary of State for the Foreign and Commonwealth Office is the minister responsible for oversight of the Government Communication Headquarters ("GCHQ"), the UK's signals intelligence agency.
3. These proceedings concern the infection by GCHQ of individuals' computers and mobile devices on a widespread scale to gain access either to the functions of those devices - for instance activating a camera or microphone without the user's consent - or to obtain stored data. Recently-disclosed documents suggest GCHQ has developed technology to infect individual devices, and in conjunction with the United States National Security Agency ("NSA"), has the capability to deploy that technology to potentially millions of computers by using malicious software ("malware"). GCHQ has also developed malware, known as "WARRIOR PRIDE", specifically for infecting mobile phones.
4. The use of such techniques is potentially far more intrusive than any other current surveillance technique, including the interception of communications. At a basic level, the profile information supplied by a user in registering a device for various purposes may include details of his location, age, gender, marital status, income,

ethnicity, sexual orientation, education, and family. More fundamentally, access to stored content (such as documents, photos, videos, web history, or address books), not to mention the logging of keystrokes or the covert and unauthorised photography or recording of the user and those around him, will produce further such information, as will the ability to track the precise location of a user of a mobile device. If the interception of communications is the modern equivalent of wire-tapping, then the activity at issue in this complaint is the modern equivalent of entering someone's house, searching through his filing cabinets, diaries and correspondence, and planting devices to permit constant surveillance in future, and, if mobile devices are involved, obtaining historical information including every location he visited in the past year. The only differences are the ease and speed with which it can be done, the ease of concealing that it has been or is being done, and the fact that, if a mobile device has been infected, the ongoing surveillance will capture the affected individuals wherever they are.

5. Moreover, the result of the installation of the malware may be to leave the devices more vulnerable to attack by third parties (such as credit card fraudsters), thereby risking the user's personal data more broadly. It is the modern equivalent of breaking in to a residence, and leaving the locks broken or damaged afterwards.
- 5A. Further, the techniques used are not passive in nature. They involve an active intrusion into a computer system or network, and the same techniques can be used to amend, add, modify or delete data or programs on a computer and to instruct it to act or respond differently to commands.
6. That conduct therefore engages Articles 8 and 10 of the European Convention on Human Rights ("ECHR"), which require (i) that the interference be "*in accordance with the law*" or "*prescribed by law*", or in other words that there be a clear and ascertainable legal regime in place which contains sufficient safeguards against abuse of power and arbitrary use, and (ii) that the interference be necessary in a democratic society and a proportionate means of achieving a legitimate aim.
7. GCHQ has not identified any legal basis for the alleged conduct, which if performed by a private individual would involve the commission of criminal offences. It is assumed at this stage that the justification under domestic law is a warrant issued

under s.5 Intelligence Services Act 1994 ("ISA 1994"), which permits "entry on or interference with property or with wireless telegraphy" in certain circumstances.

8. Even if there is such a justification, it is nevertheless clear that (i) the interference with Convention rights is not "in accordance with the law" or "prescribed by law", since there is no public legal regime in place that is capable of meeting the requirements of Articles 8 and 10, and (ii) it is not proportionate, both because of the extremely serious nature of the intrusion, and because the relevant activity (at least the infection of the devices, if not the use of the malware once installed) appears to be indiscriminate in nature.
9. These grounds accompany the forms T1 and T2 filed by Privacy International. They set out, in summary terms, the grounds relied upon. Privacy International will make detailed submissions and serve evidence in due course, once the Defendants have clarified the nature of their activities and their justification for them.
10. Privacy International also seeks a public hearing of its complaint. The fact that documents evidencing the Defendants' activities have been released into and extensively reported on and analysed in the public domain means that there is no longer any good reason to uphold the Defendants' ordinary policy of 'neither confirm nor deny' in this case: see *R (Bancoult) v SSFCA* [2013] EWHC 1502 (Admin) at [28].

THE DEFENDANTS' CONDUCT

11. From June 2013 onwards, a number of public disclosures have been made (beginning with publication in *The Guardian* and *The Washington Post* of documents leaked by a former NSA contractor, Edward Snowden) about programmes of surveillance operated by the NSA with the close involvement of other authorities, including the UK authorities and specifically GCHQ.
12. Most of the revelations concern the scope of the NSA and GCHQ's monitoring of communications, including the "Prism" programme (the monitoring of information stored by telecommunications companies or internet service providers) and "upstream collection" (the direct interception of communications during transmission). Those activities are the subject of existing complaints before the IPT.

13. This complaint relates to more recent revelations regarding GCHQ's infection and intrusion into individual devices.
14. For instance, on 12 March 2014, *The Intercept* – an online publication established in February 2014 with the aim, among others, of reporting on and analysing documents released by Edward Snowden – published an article entitled “*How the NSA Plans to Infect ‘Millions’ of Computers with Malware.*”¹ Published along with that article were numerous documents and excerpts of documents indicating that the NSA “*is dramatically expanding its ability to covertly hack into computers on a mass scale by using automated systems that reduce the level of human oversight in the process. The classified files – provided previously by NSA whistleblower Edward Snowden – contain new details about groundbreaking surveillance technology the agency has developed to infect potentially millions of computers worldwide with malware ‘implants.’*” GCHQ has collaborated with the NSA in these activities.
15. By way of summary of what is now publicly known:
 - a. GCHQ has worked closely with the NSA to intrude on individual computers and mobile devices. This is evidenced in *The Intercept* article, which both describes GCHQ's intrusion efforts, and includes a number of excerpts of documents marked with security designations showing they were shared with all the members of the Five Eyes alliance, including the NSA and GCHQ. The NSA and GCHQ's close working relationship is now well documented, including that many of their agents are issued access cards that allow them to enter the facilities of either agency.
 - b. One of the documents published by *The Intercept* describes the technique of implanting malware onto a user's computer as “Active SIGINT”, and says: “*Active SIGINT offers a more aggressive approach to SIGINT. We retrieve data through intervention in our targets' computers or network devices. Extract data from machine.*”²

¹ <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>

² <https://prod01-cdn02.cdn.firstlook.org/wp-uploads/sites/1/2014/03/intelligent-command-and-control.jpg>

- c. That technique involves covert installation of software onto the user's computer through one of a number of means, such as tricking the user into clicking a malicious link, or (more recently) injecting malicious code into the network transmission that individuals receive when browsing websites like Facebook or LinkedIn so as to transfer the malware as part of the computer's ordinary downloading of data.
- d. *The Intercept* also reports: "GCHQ, the British intelligence agency, appears to have played an integral role in helping to develop the implants tactic."³ (underlining indicates emphasis added). Some of these intrusion tools developed are as follows: "An implant plug-in named CAPTIVATEDAUDIENCE, for example, is used to take over a targeted computer's microphone and record conversations taking place near the device. Another, GUMFISH, can covertly take over a computer's webcam and snap photographs. FOGGYBOTTOM records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts. GROK is used to log keystrokes. And SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer."
- e. In addition to the concept of implanting malware itself, the documents released by *The Intercept* describe an automated system named TURBINE which, in the words of the above undated document, "will allow the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually."⁴ Another undated document reads: "TURBINE [...] will increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CAN) implants to potentially millions of implants."⁵ Yet another, shared with the Five Eyes surveillance alliance, referred to TURBINE as permitting "Industrial-scale exploitation."⁶
- f. Images of slides from a leaked presentation prepared by the NSA's "Turbulence" team in August 2009 describe the "Expert System" which is

³ <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>

⁴ <https://prod01-cdn02.cdn.firstlook.org/wp-uploads/sites/1/2014/03/intelligent-command-and-control.jpg>

⁵ <https://prod01-cdn03.cdn.firstlook.org/wp-uploads/sites/1/2014/03/turbine-large.jpg>

⁶ <https://firstlook.org/theintercept/document/2014/03/12/industrial-scale-exploitation/>

designed to manage the implants and “decide” how best to extract data. The classification on those slides (“TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123”) indicates that they were shared with the UK authorities among others, and the diagram of the Expert System shows that a station at “MHS” in the UK, i.e. RAF Menwith Hill station, is part of the network.⁷

- g. Further documents show that RAF Menwith Hill and GCHQ have been integral to the development and use of implanting techniques.
 - i. A document shared with the Five Eyes alliance refers to MHS as having tested the use of a technique (called “Quantum”) in relation to Yahoo and Hotmail, websites which host online email accounts on behalf of private users.⁸
 - ii. Another such document refers to the availability of that technique at sites including “Menwith Hill Station” and “INCENSOR (DS-300) – with help from GCHQ”.⁹
 - iii. *Der Spiegel*, reporting on 29 December 2013 on an internal NSA document disclosed to it, wrote: “A comprehensive internal presentation titled ‘QUANTUM CAPABILITIES’, which SPIEGEL has viewed, lists virtually every popular Internet service provider as a target, including Facebook, Yahoo, Twitter and Youtube. ‘NSA QUANTUM has the greatest success against Yahoo, Facebook and static IP addresses,’ it states. The presentation also notes that the NSA has been unable to employ this method to target users of Google services. Apparently, that can only be done by Britain’s GCHQ intelligence service, which has acquired QUANTUM tools from the NSA.”

16. In addition to the above, there is clear evidence that GCHQ has developed extensive means of manipulating mobile devices in particular:

⁷ <https://firstlook.org/theintercept/document/2014/03/12/turbine-turmoil/>

⁸ <https://firstlook.org/theintercept/document/2014/03/12/menwith-hill-station-leverages-xkeyscore-quantum-yahoo-hotmail/>

⁹ <https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/>

- a. Documents published by *The Guardian* on 28 January 2014, in particular a set of slides from a GCHQ presentation delivered on 28 May 2010, revealed that GCHQ had by May 2010 developed a suite of software known as "WARRIOR PRIDE" for iPhones and Android devices.
- b. The slides referred to the following functionality available in relation to those devices, with their codenames:

*** Power Management - DREAMY SMURF*

** Hot mic - NOSEY SMURF*

** High precision GEO - TRACKER SMURF*

** Kernel stealth - PORUS*

** Self protection - PARANOID SMURF*

** File retrieval - any content from phone, e.g. SMS, MMS, e-mails, web history, call records, videos, photos, address book, notes, calendar, (if its on the phone, we can get it)"*

- c. In other words, as early as May 2010 those tools allowed at least for (i) the activation of a microphone and the taking of recordings without the user's consent ("Hot mic"), (ii) precise identification of the geographical whereabouts of the user ("High precision GEO"), (iii) avoidance of detection that the security of the device has been compromised ("Kernel stealth" and "Self-protection"), and (iv) the retrieval of any content on the phone.

17. It is not known (not least because there is no clear or accessible legal regime governing it) how many devices are infected, whether there is any time limit on the infection, who has the power to activate or use the malware, who has access to the information it generates, and so on. That is itself a significant cause for concern. But in any event there are two other concerns as a matter of principle:

- a. First, however widely they are used, the tools allow GCHQ access to a large amount of highly private data. The information stored on a computer or mobile device is potentially far more comprehensive than the information

that an individual communicates over a network in a manner capable of interception, or information that could be obtained from a search of his home or office. Indeed, computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, correspondence files, fixed-line telephones. Increasingly, they are also replacing our formal identification documents, our bank and credit cards. These devices may contain not only details about the user's personal circumstances (for instance his age, gender, or sexual orientation), but also financial information, unencrypted passwords, privileged legal information and so on. Unlike in the case of an interception of communications, even information that the user deems too personal, private or sensitive to communicate is vulnerable to collection or monitoring when intrusion tools are utilised. And, as noted, intrusive malware not only gives access to historical, current and future data stored on these devices, but also grants the person who planted the malware total control over the device. This means that any functionality on the device, including its camera, microphone, or word processing and storage software, may be utilized and manipulated. Additionally, access to an electronic device enables ~~the~~ whoever controls the malware to obtain data that is situated not on the device itself, but in an external network server known as "the cloud". For example, while only a limited number of emails might be stored directly on an individuals' smart phone, control of that smart phone enables access to all emails stored in the cloud.

- b. Second, the means by which collection or monitoring is made possible may itself leave users vulnerable to further damage, in three ways. First, the malware that is installed on a device could be used by third parties; for example, the keyloggers described above might be used to capture a person's credit card number. Second, the changes necessary to install the malware without alerting the user or his security software may result in security vulnerabilities that could be exploited by third parties in other ways. Third, to the extent that any exploits are built into network infrastructure in order to enable the installation of the malware, those exploits might themselves be used by third parties to similar ends.

18. Further, there have been clear indications that GCHQ itself has reservations about the legality of such operations.

- a. An undated NSA document referring to a trilateral programme between “NSA, GCHQ, and FRA” (the Swedish signals intelligence agency) for the deployment of the Quantum technique says: “Continued GCHQ involvement may be in jeopardy due to British legal/policy restrictions”.³⁰ There is no further explanation of the concerns.
- b. A document prepared by a representative of GCHQ for an international telecommunications conference in September 2010 reads, in relation to the implanting of software to decrypt communications encrypted with a particular standard (“MIKEY-IBAKE”): “An additional concern in the UK is that performing an active attack, such as the Man-in-the-Middle attack proposed in the Lawful Interception solution for MIKEY-IBAKE may be illegal. The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material. A Man-in-the-Middle attack causes modification to computer data and will impact the reliability of the data. As a result, it is likely that LEMFs and PLMNs would be unable to perform LI on MIKEY-IBAKE within the current legal constraints.”

Effect on Privacy International

19. In order to pursue this complaint, Privacy International need not show that it has actually been the subject of the alleged interference.

- a. In the context of monitoring of communications, the European Court of Human Rights has held that “the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and

³⁰ <https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html>

thereby amounts in itself to an interference with the exercise of the applicants' rights under art.8, irrespective of any measures actually taken against them": Liberty v United Kingdom (2009) 48 EHRR 1 at [56].

- b. For the reasons given above, the interference in the present case – the active collection of data through manipulation of the user's property – is more serious than the monitoring of communications. Accordingly, the same principle applies in this case.
 - c. Likewise, if "the mere existence of legislation" permitting interference is a sufficient interference with a fundamental freedom to justify a legal challenge, then the fact that there is evidence of an interference without any meaningful legislative control is an even clearer case where a complainant need not show actual interference with his own affairs. In those circumstances, where there is no statutory scheme, Code of Practice or published policy indicating who can be targeted and in what circumstances, it is even more difficult for an individual to know whether they have been subject to the relevant activity.
 - d. The same principle was applied to Article 10 by the Court in Weber v Germany (2008) 46 EHRR SE5 at [145], where the applicant's status as a journalist meant that surveillance of communications affected her right to freedom of expression: she "communicated with persons she wished to interview on subjects such as drugs and arms trafficking or preparations for war, which were also the subject of strategic monitoring. Consequently, there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone." Again, the test is only whether the complainant is within the category of persons who may be affected by the interference.
20. Privacy International is clearly within the category of persons who may be affected by the interference.
- a. It and its staff routinely use a variety of computers and mobile devices in the course of their work, including smartphones such as those identified in GCHQ's May 2010 presentation described above. Given the apparently

indiscriminate nature of the activity in question, that is sufficient on its own to place them in the necessary category.

- b. Even if the activity is not wholly indiscriminate, it is clearly wide-ranging. Privacy International, as an organisation campaigning against excessive state surveillance (and therefore critical of the activities of GCHQ), and corresponding with other organisations and campaign groups across the world with similar goals and objectives, is well within the potential scope of such activity.
- c. Moreover, Privacy International has precisely the same concern as the applicant in *Weber* in relation to Article 10. It works on capacity building on issues of privacy in developing countries, sometimes in places with weak democracies which are of particular interest to US and UK foreign policy, and where strong privacy safeguards may conflict with the objectives of intelligence agencies. Groups and individuals in repressive regimes, individuals in the UK concerned about their own privacy, as well as victims, whistleblowers and journalists frequently contact Privacy International. They may be dissuaded from doing so, or from communicating freely, for fear that their communications will be monitored.

LEGAL FRAMEWORK

Human Rights Act 1998 and European Convention of Human Rights

21. By s.6 Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates various rights from the European Convention including Articles 8 and 10.
22. Article 8 of the Convention provides:
 1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
 2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a*

democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 10 provides:

1. *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

23. There are therefore four questions in any analysis of whether those rights have been breached:

- a. Is the relevant right engaged?
- b. Is the interference "*in accordance with the law*" (Article 8) or "*prescribed by law*" (Article 10)?
- c. Is the interference in pursuit of one of the listed aims?
- d. Is the interference "*necessary in a democratic society*" in pursuit of that aim – in other words, is it proportionate to the goal which is sought to be achieved?

24. Article 8 and Article 10 rights are clearly engaged by the interference.

- a. As for Article 8, the collection of data through implanted malware on computers and mobile devices has the potential, in the modern world, to

reveal almost every intimate detail of a person's life – from correspondence and connections, to historical and current location, to financial and health information, to information about family life, sexuality, or political beliefs – and may allow real-time surveillance through keystroke logging or the co-option of microphones and video cameras. All of these things are obviously private information within the meaning of Article 8. By way of example, the European Court of Human Rights has held in the context of workplace monitoring that that “*emails sent from work*” and “*information derived from the monitoring of personal internet usage*” are both protected by Article 8: Copland v United Kingdom (2007) 45 EHRR 37 at [41]. That is a small subset of the information that can be obtained through GCHQ's activity.

- b. As for Article 10, the Court has recognised in Weber (above, [144-145]) that the fact that “*the threat of secret surveillance [...] necessarily strikes at the freedom of communication of users of telecommunications services*” means that it engages Article 10 if the effect is to discourage communications. The same principle must apply to the threat of intrusion into computers and devices via the internet, to the extent that it discourages the free use of the internet, which it obviously will if left uncontrolled.

- 25. Privacy International accepts that, in principle, surveillance may be conducted for legitimate aims such as national security. The issue is therefore whether the interference is “*in accordance with the law*” or “*prescribed by law*”, and whether it is necessary and proportionate.
- 26. The requirement that the interference be “*in accordance with the law*” or “*prescribed by law*” demands more than merely that the interference be lawful as a matter of English law, and it must also be “*compatible with the rule of law*”: Gillan v United Kingdom (2010) 50 EHRR 45 at [76]. That means it must “*afford a measure of legal protection against arbitrary interferences by public authorities*”, and indicate “*with sufficient clarity*” the scope of any discretion conferred and the manner of its exercise: Gillan at [77].
- 27. Numerous cases have addressed the “*in accordance with the law*” requirement in the context of secret surveillance and information gathering.

- a. In *Malone v United Kingdom* (1985) 7 EHRR 14, the Court held that the legal regime governing interception of communications “must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence” [67]. It must be clear “what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive” and the law must indicate “with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities” [79].
- b. In *Association for European Integration and Human Rights v Bulgaria* (62540/00, 28 June 2007), the Court held at [75]: “In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated [...]”.
- c. These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the “procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material” (*Liberty v UK* (2009) 48 EHRR 1 at [69]).
- d. In *Weber* the ECHR held at [93-94]: “The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures [...] Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.”
- e. The Court continued in *Weber* by setting out the matters which any legal regime governing secret surveillance must expressly address in statute in order to be regarded as lawful:

95 In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.

28. These principles apply with equal effect to the requirement in Article 10 that the interference be “in accordance with the law” (see, for example, *Weber*, at paragraph 147, and *Sunday Times v United Kingdom* (1979) 2 EHRR 245, at paragraphs 48 and 49).

Domestic legal regime governing the relevant conduct

Regulation of Investigatory Powers Act 2000

29. RIPA 2000 regulates, among other things, the interception of communications in the course of transmission (Part I Chapter I), the acquisition of communication data from persons providing a telecommunication service (Part I Chapter II), and intrusive surveillance and covert human intelligence sources (Part II), in the UK.
30. Part I Chapter I empowers the Secretary of State to issue warrants for the interception of communications under s.5, if he considers the interception necessary on a number of listed grounds, including national security, and proportionate to the aim to be achieved.
31. Section 2(2) RIPA 2000 defines “interception” as follows:

“a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he –

(a) so modifies or interferes with the system, or its operation,

(b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."

32. That might extend to some of the effects of the conduct at issue in this complaint – for instance, if malware were implanted and then used in order to record a phone call while it is being made – but it does not cover most of the functions described in the leaked documents. For example, the extraction of documents from a hard disk or a mobile device would not be the interception of a communication in the course of its transmission; it might involve the collection by GCHQ of information which the affected individual never intended to share with anyone. Likewise, the ability to activate a user's camera or microphone without his knowledge would not involve the interception of any communication. Accordingly, it cannot be said that the implanting of malware is merely a modification "*so [...] as to make some or all of the contents of the communication available while being transmitted*".
33. RIPA Part I Chapter II covers the acquisition and disclosure of "*communication data*", namely data held by a person providing a telecommunication service (section 21(4)). That is clearly not engaged.
34. Part II is not engaged either; s.48(3) provides that "*References in this Part to surveillance do not include references to [...] (c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under – (i) section 5 of the Intelligence Services Act 1994 [...]*". In a case involving interference with property by GCHQ, which (as set out below) is governed by the Intelligence Services Act 1994, that exemption applies. In any event, nowhere in Part II is there any reference to the manipulation of electronic devices belonging to others; the Act is clearly aimed at a different kind of information-gathering, its interpretation provisions referring to "*monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications*", either by officials alone or "*by or with the assistance of a surveillance device*" (s.48(2)), and only in certain circumstances "*the interception of a communication in the course of its transmission*". As an interference with fundamental rights it cannot lightly be construed as covering an entirely different kind of information-gathering: *R (Simms) v SSHD* [2000] 2 AC 115. In any event, it does not even arguably extend to activity such as the collection and extraction of documents.

35. It is an offence under s.1(1) Computer Misuse Act 1990 ("CMA 1990") to cause a computer to perform any function with intent to secure access to any program or data held in it, or to enable any such access to be secured, if the access is unauthorised and known to be unauthorised. (The term "computer" is not defined in the Act, but in another statutory context was held by Lord Hoffmann in *DPP v McKeown* [1997] 1 WLR 295 to mean "a device for storing, processing and retrieving information". Modern mobile devices, which are far more sophisticated than the desktop computers available when the Act was passed, would surely qualify.)
36. Further, under s.3 CMA 1990 it is an offence to do any unauthorised act in relation to a computer, in the knowledge that it is unauthorised, if (i) the intention is to impair the operation of the computer, to prevent or hinder access to any program or data, to impair the operation of any program or the reliability of any data, or to enable any of those things, or (ii) the perpetrator is reckless as to whether the act will do any of those things. S.3(5) clarifies that the relevant effects may be only temporary, and also that a reference to doing an act includes a reference to causing an act to be done. The result is that the infection of a computer pursuant to an automated process would still be an offence on the part of the person who commenced or directed that process. The intrusion at issue here impairs the operation of the target computers in multiple ways, including by draining battery life and using bandwidth and other computer resources.
37. Prior to recent amendments (as to which see below), s.10 CMA 1990 provided that section 1(1) "has effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and (b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure." However, this override does—did not apply to section 3(1). Accordingly, the s.3 offence had effect regardless of any other enactment relating to powers of inspection/examination, search or seizure. Therefore, at least to the extent that such activities occur in England and Wales, any GCHQ activities that impair the operation of a computer - for instance, by leaving it vulnerable to future exploitation, as explained above - were prima facie unlawful, notwithstanding any provision in another enactment purporting to authorise them.

37A. On 3 March 2015, the Serious Crime Act 2015 received Royal Assent. Section 44 of the 2015 Act amends s. 10 CMA 1990. The amended version now provides:

"Sections 1 to 3A have effect without prejudice to the operation-

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or any other enactment by virtue of which the conduct in question is authorised or required"

37B. These amendments (which are not retrospective) were brought into force on 3 May 2015.

37C. Paragraph 139 of the Explanatory Notes to the Serious Crime Act 2015 purport to provide an explanation of the effect of the amendments:

"Section 10 of the 1990 Act contains a saving provision. It provides that the offence at section 1(1) of the 1990 Act has effect without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure; and in Scotland of any enactment or rule of law relating to powers of examination, search or seizure. The amendment to section 10 of the 1990 Act made by this section is a clarifying amendment. It is designed to remove any ambiguity over the interaction between the lawful exercise of powers (wherever exercised) conferred under or by virtue of any enactment (and in Scotland, rule of law) and the offence provisions. "Enactment" is expressly defined to provide certainty as to what this term includes. The title of section 10 of the 1990 Act has also been changed to remove the reference to "certain law enforcement powers" (see paragraph 12 of Schedule 4). This is to avoid any ambiguity between the title and the substance of that section."

37D. The jurisdictional effect of the CMA 1990 is governed by two sets of statutory provisions. Section 4 of the CMA 1990 provides:

"(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1, 3 or 3ZA above-

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned¹¹; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

Subject to sub-section (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed."

37E. A significant link with domestic jurisdiction is dealt with by s. 5 CMA 1990:

- a. Under sub-section (1A) there is a significant link with domestic jurisdiction if the accused was a UK national and the act constituted an offence under the law of the country in which it occurred.
- b. Under sections 1 and 3, there is a significant link with domestic jurisdiction if the accused was in the home country, and so was the relevant computer.

37F. The effect of these territorial provisions is modified by s. 31 of the Criminal Justice Act 1948, which extends the scope of territorial jurisdiction provisions in certain cases involving Crown servants:

"(1) Any British subject employed under His Majesty's Government in the United Kingdom in the service of the Crown who commits, in a foreign country, when acting or purporting to act in the course of his employment, any offence which, if committed in England, would be punishable on indictment, shall be guilty of an offence and subject to the same punishment, as if the offence had been committed in England."

Intelligence Services Act 1994

38. S.3 ISA 1994 provides the statutory basis for GCHQ and delineates its statutory functions. Those functions include "to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide [to various organisations] information derived from or related to such emissions or equipment and from encrypted material". By s.3(2) those functions are exercisable only in the

¹¹ The "home country concerned" is defined as being England and Wales, Scotland or Northern Ireland as appropriate - section 4(6) CMA 1990.

interests of national security, the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime.

39. S.4(2) requires the Director of GCHQ to ensure *“that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings.”*
40. S.5(1) provides: *“No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.”* The Secretary of State may issue such a warrant on the application of GCHQ in respect of any action, provided he *“thinks it necessary for the action to be taken for the purpose of assisting [...] GCHQ in carrying out [its statutory functions],”* *“is satisfied that the taking of the action is proportionate to what the action seeks to achieve”*, and is satisfied that satisfactory arrangements are in force with respect to section 4(2) in relation to onward disclosure.
41. In other words, the apparent legal basis for the activity at issue in this complaint is an extremely broad power on the part of the Secretary of State to render lawful what would otherwise be unlawful.

GROUND 1: IN ACCORDANCE WITH LAW / PRESCRIBED BY LAW

41A In order to be “in accordance with the law”, relevant activity must have a legal basis in domestic law, and also contain sufficient protections against arbitrary conduct so as to ensure that intrusive powers are exercised properly.

41B The carrying out of CNE is not in accordance with domestic law. First, pPrior to the coming into force of the Serious Crime Act 2015;

- a. Any conduct by the Respondents amounting to a breach of s. 3 of the CMA 1990 could not, by virtue of s. 10 CMA 1990, be authorised pursuant to a warrant issued under RIPA or the ISA. Only lesser interferences, amounting to a breach of s. 1 CMA 1990 only, could be authorised by warrant. This position reflected a legislative decision that whilst state-sanctioned operations that gain unauthorised access to a computer system should be lawful if supported by some other enactment, operations that have an adverse effect on the computer system or which modify data should not be permitted in any circumstances. Such conduct amounts potentially to an active and harmful attack on a computer system or network, and could include warlike operations.
- b. Further, any breach of any provisions of the CMA 1990 by a Crown servant abroad is deemed to have taken place in England, and is within the territorial jurisdiction of the CMA 1990. Any such conduct, except to the extent capable of being authorised and in fact authorised by a valid warrant, was and is unlawful.

41C. Second, s.5 ISA 1994 empowers the Secretary of State to issue a warrant in respect of “such action as is specified in the warrant in respect of any property so specified”. That is narrower than s.7 ISA 1994, which provides that an otherwise unlawful act is not unlawful if “the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State”. As a result of the requirement that the action and property both be “specified”, the Secretary of State is not empowered to issue ‘thematic’ or ‘class’ warrants. Any such warrants which have been issued are unlawful, and the acts purportedly authorised by them were also unlawful.

41D. Third, the power to issue a warrant in respect of interference with "property" does not extend to interference with intangible legal rights, such as copyright. It is limited to physical property, as is clear from the fact that s.5(3) and (3A) refer to "property in the British Islands". Any warrants which have been issued concerning interference with intangible legal rights are unlawful and the acts purportedly authorised by them were also unlawful.

41E. To the extent that any CNE has involved interference with copyright, that interference is a derogation from Article 2 of Directive 2001/29 and must also be shown:

- a. to fall within one of the exceptions in Article 5.2 or 5.3, strictly construed (C-5/08 *Infopaq International A/S v Danske Dagblades Forening* ECLI:EU:C:2009:465);
- b. not to conflict with the normal exploitation of the work or unreasonably to prejudice the legitimate interests of the rightholder (Article 5.5); and,
- c. to be proportionate to the legitimate aim, surviving the "relatively intensive and thorough review" which is to be applied in challenges to measures that interfere with copyright: *R (BASCA) v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin) at [135].

41F. The standard required to justify a derogation from EU law rights in the context of surveillance was set out by the Grand Chamber of the CJEU in Case C-293/12 *Digital Rights Ireland*.

42. Further, and in any event, CNE operations are not accompanied by sufficient protections against arbitrary conduct so as to be in accordance with the law. As already indicated, the activities in question have the potential to be more intrusive than any other form of surveillance or data-gathering. The amount of information stored on mobile phones and computers is vast, and much of it will be highly personal in nature.

43. Unlike the monitoring of communications, these activities enable GCHQ to obtain that information whether or not the affected individual has ever chosen to share it with anyone. Moreover, the logging of keystrokes and the covert activation of

cameras and microphones enable GCHQ to obtain further potentially sensitive information whether or not the affected individual has ever chosen even to store it. In addition, CNE operations may include active alteration and amendment of programs and data on a computer system, and steps that effect the operation or reliability of the computer, or a computer network.

44. A user may not even know of the full extent of what his computers or mobile devices store. A mobile phone may, for instance, log all his historical geographical movements as well as his current location. For instance, if he went for a job interview or a medical appointment during work hours, that would be logged regardless of whether there were any other record of that interview or appointment having been arranged.

45. Further:

- a. the fact that computers and devices are vulnerable to intrusion in this way will inevitably discourage people from using the internet freely, and in particular those individuals and organisations who may have wished to correspond with Privacy International about legitimate activity in the sphere of privacy protection;
- b. the potential vulnerabilities resulting from the forcible infection of devices and the necessary weakening of security that such manipulation involves have the potential to produce further interferences beyond those which GCHQ directly controls;
- c. the potential for GCHQ to take over a compromised device altogether, potentially altering its contents or altering its mode of operation or behaviour, including leaving potential vulnerabilities, raises serious concerns about the integrity of any evidence from such sources that might be used in legal proceedings, and the mechanisms would should be established and enforced in order to ensure that that integrity is protected;
- d. as a matter of general principle, the fact that computer hacking involves sophisticated technology and concepts which were unknown 20 years ago strongly militates in favour of a requirement that it be governed by an

appropriate legal framework developed with that technology and those concepts in mind.

46. Accordingly, it is if anything more necessary than in an ordinary 'interception' case that there be a clear legal framework governing activities of this sort.

47. There is no such framework. The only statutory scheme dealing expressly with the unauthorised infection of computers was established in 1990. Far from establishing a Convention-compliant framework within which such infection is to be permissible on certain conditions and with certain safeguards, it makes clear that GCHQ's activity is simply unlawful in the absence of a supervening provision. The availability of a warrant under ISA 1994 that simply cancels any unlawfulness is self-evidently not an adequate safeguard.

47A. Further, it is unclear whether:

- a. the Respondents contend that a warrant is always required to carry out CNE operations abroad, or over a foreign computer, even if the relevant user is located in the United Kingdom;
- b. whether the Respondents contend that a class authorisation by the Secretary of State is lawful, without a specific and individual warrant being made in each case of intrusion; and
- c. whether proper and complete records, together with an analysis of necessity and proportionality is kept in each case of CNE. The report of the Intelligence and Security Committee suggests that such records are not kept, indicating that meaningful oversight of such operations is impossible.

48. There is no Code of Practice governing the circumstances in which intrusion will be permitted, by what means, against whom, in response to what level of suspicion and for what kind of misconduct, or for how long their systems will be permitted to remain compromised.¹² Nor is there anything governing the procedure to be

¹² A draft Equipment Interference Code of Practice was published for consultation on the same date as the Defence was served, presumably in response to the allegations made in this case. The outcome of the consultation is not known, and any draft Code must be approved by an affirmative resolution of both Houses of Parliament. The Claimant has lodged representations on the draft Code, a copy of

followed in selecting for examination, sharing, storing and destroying any material obtained (*Liberty* at [69]), or anything governing the relationship between GCHQ's programme and the equivalent programmes being pursued by the NSA, FRA, and potentially others. Even if it is strictly speaking permissible as a matter of construction of domestic law (which, given the Defendants have not yet advanced any such case, is not admitted), it falls short of the requirements of the rule of law and of Articles 8 and 10 of the Convention.

GROUND 2: DISPROPORTIONALITY OF INTERFERENCE

49. Given the limited availability of the details of GCHQ's activity (still less the purported legal basis for it) to Privacy International at this stage, Privacy International must reserve the right to make more detailed submissions on the disproportionality of the interference in due course.
50. For present purposes it is sufficient to say that the nature of the interference, as set out above, is far more serious than the interception of communications and, if left unchecked, amounts to one of the most intrusive forms of surveillance any government has conducted. In allowing GCHQ to extract a huge amount of information (current and historical), much of which an individual may never have chosen to share with anybody, and to turn a user's own devices against him by co-opting them as instruments of video and audio surveillance, it is at least as intrusive as searching a person's house and installing bugs so as to enable continued monitoring. In fact, it is more intrusive, because of the amount of information now generated and stored by computers and mobile devices, the speed, ease and surreptitiousness with which surveillance can be conducted, and because it allows the ongoing surveillance to continue wherever the affected person may be. Further, the operation of the computer or device and the data stored on it can be altered or modified. In those circumstances any justification would have to be extremely specific and compelling in order to render that activity proportionate to any legitimate aim. All the indications so far are that the activity goes far beyond any such justification.

which is attached. In the event that the Code is made in the form of the draft Code, the Claimant will rely on its representations.

51. Furthermore, such intrusion into “millions” of devices is highly unlikely to be proportionate to any legitimate aim even if logic has been applied to the selection of those devices. If, as is more likely, GCHQ has simply taken advantage of its tools in order to infect large numbers of devices near-indiscriminately, then it will be even more obviously disproportionate.
52. Moreover, the lack of safeguards mentioned above – in particular the apparent lack of any restriction on the extent or duration of the infection of any particular device – tends strongly against any finding that the interference is proportionate to any legitimate aim.
- 52A. The question of proportionality arises primarily by reference to Articles 8 and 10 ECHR. However, to the extent that any CNE has involved interference with copyright, that interference is a derogation from Article 2 of Directive 2001/29 and must also be shown:
- a. to fall within one of the exceptions in Article 5.2 or 5.3, strictly construed (C-5/08 *Infopaq International A/S v Danske Dagblades Forening* ECLI:EU:C:2009:465);
 - b. not to conflict with the normal exploitation of the work or unreasonably to prejudice the legitimate interests of the rightholder (Article 5.5);
 - c. to be proportionate to the legitimate aim, surviving the “relatively intensive and thorough review” which is to be applied in challenges to measures that interfere with copyright: *R (BASCA) v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin) at [135]; and
 - d. to comply with the safeguards identified by the Grand Chamber of the CJEU in Case C-293/12 *Digital Rights Ireland*.

CONCLUSION

53. Privacy International seeks the following orders (which, again, may have to be supplemented or amended in light of further disclosures):

- a. A declaration that GCHQ's intrusion into computers and mobile devices is unlawful and contrary to Articles 8 and 10 ECHR;
- b. An order requiring the destruction of any unlawfully obtained material;
- c. An injunction restraining further unlawful conduct.

BEN JAFFEY

TOM CLEAVER

19 May 2015

13 July 2015

IN THE INVESTIGATORY POWERS TRIBUNAL

BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Defendants

RE-AMENDED STATEMENT OF GROUNDS

INTRODUCTION

1. The Claimants provide internet and communications services. They are referred to below as the "internet and communications service providers". They are based in various countries, including the UK. Collectively, they each provide a variety of services including internet access, email services, and website hosting.
 - a. The First Claimant ("GreenNet") is a limited company active since 1986 and owned by the GreenNet Educational Trust, a charity registered in England & Wales.
 - b. The Second Claimant ("Riseup") is a registered non-profit organisation based in Seattle, Washington, and active since 2000.
 - c. The Third Claimant ("Mango Email Service") is a non-profit association in Zimbabwe and active since 1988.
 - d. The Fourth Claimant ("Jinbonet") is a registered non-profit in South Korea, and active since 1988.

- e. The Fifth Claimant ("Greenhost") is a company registered in the Netherlands and active since 2001.
 - f. The Sixth Claimant ("May First/People Link") is a registered non-profit organisation based in Brooklyn, New York and active since 2005.
 - g. The Seventh Claimant ("Chaos Computer Club") is a registered non-profit organisation based in Hamburg, Germany, and active since 1981.
2. The Secretary of State for Foreign and Commonwealth Affairs is the minister responsible for oversight of the Government Communication Headquarters ("GCHQ"), the UK's signals intelligence agency.
 3. These proceedings concern GCHQ's apparent targeting of internet and communications service providers in order to compromise and gain unauthorised access to their network infrastructures in pursuit of its mass surveillance activities. The claims set out below arise out of reports, published by the German newspaper *Der Spiegel*, that GCHQ has conducted targeted operations against internet service providers to conduct mass and intrusive surveillance.
 4. In late 2013, *Der Spiegel* reported that GCHQ had attacked Belgacom, the Belgian telecommunications group, so as to enable it to engage in surveillance of users of Belgacom's network. The documents seen by *Der Spiegel* indicate that the attack "was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a 'Quantum Insert' ('QI'). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware [malicious software] on their computers that can then manipulate them."¹ It is important to note that the employees of Belgacom were not targeted because they posed any legitimate national security concern. Instead, they were subject to intrusive surveillance because they held positions as administrators of Belgacom's networks. By hacking the employees, GCHQ could secure access to the customers. Once employees' computers were compromised, *Der Spiegel* reported, "GCHQ continued to probe the areas of infrastructure to which the targeted employees had access [...]." Reportedly, GCHQ were "on the verge of accessing the Belgians' central roaming

¹ <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html>

router. The router is used to process international traffic. According to the presentation, the British wanted to use this access for complex attacks ("Man in the Middle" attacks) on smartphone users." A "Man in the Middle" attack is a technique for bypassing modern encryption software. It operates by interposing the attacker (here, GCHQ) between two computers that believe that they are securely communicating with each other. In fact, each is communicating with GCHQ, who collect the communications, as well as relaying them in the hope that the interference will be undetected.

5. *Der Spiegel* has further reported that the attack on Belgacom was "not an isolated case, but in fact is only one of the signature projects of an elite British Internet intelligence hacking unit working under the auspices of a group called MyNOC".² Indeed, *Der Spiegel* subsequently reported that GCHQ targeted internet exchange points run by German companies Stellar, Cetel and IABG. Reportedly, "[t]he operation, carried out at listening stations operated jointly by GCHQ with the NSA in Bude, in Britain's Cornwall region, is largely directed at Internet exchange points used by the ground station to feed the communications of their large customers into the broadband Internet. In addition to spying on the Internet traffic passing through these nodes, the GCHQ workers state they are also seeking to identify important customers of the German teleport providers, their technology suppliers as well as future technical trends in their business sector."³ It therefore appears that use is being made of this privileged access for the purposes of economic espionage, including economic espionage directed at other companies in the EU.
6. The Claimants are legitimately concerned about such attacks, of which they may have been, or may yet be, victims. The attacks gives rise to four main legal issues.
 - a. First, in the course of such an attack, network assets and computers belonging to the internet and communications service provider are altered without the provider's consent. That is in itself unlawful under the Computer Misuse Act 1990 in the absence of some supervening authorisation. Depending on the nature and extent of the alterations, the attacks may also cause damage amounting to an unlawful interference with the internet and communications

² <http://www.spiegel.de/international/world/gchq-targets-engineers-with-fake-linkedin-pages-a-932821.html>

³ <http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html>

service provider's property contrary to Article 1 of the First Protocol ("A1P1") to the European Convention on Human Rights ("ECHR").

- b. Second, the surveillance of the internet and communications service provider's employees is an obvious interference with the rights of those employees under Articles 8 and 10 ECHR, and by extension the provider's own Article 10 rights. As *Der Spiegel* reported in relation to a separate attack on Mach, a data clearing company, a computer expert working for the company was heavily targeted: "A complex graph of his digital life depicts the man's name in red crosshairs and lists his work computers and those he uses privately ('suspected tablet PC'). His Skype username is listed, as are his Gmail account and his profile on a social networking site. [...] In short, GCHQ knew everything about the man's digital life." It is not simply a question of GCHQ confining its interest to employees' professional lives. They are interested in knowing everything about the staff and administrators of computer networks, so as to be better able to exploit the networks they are charged to protect.
- c. Third, the exploitation of network infrastructure enables GCHQ to conduct mass and intrusive surveillance on the customers and users of the internet and communications service providers' services in contravention of Articles 8 and 10 ECHR. Network exploitation of internet infrastructure enables GCHQ to undertake a range of highly invasive mass surveillance activities, including the application of packet capture (mass scanning of internet communications); the weakening of encryption capabilities; the observation and redirection of internet browsing activities; the censoring or modification of communications en route; and the creation of avenues for targeted infection of users' devices. Not only does each of these actions involve serious interferences with Article 8 ECHR rights, by creating vulnerabilities and mistrust in internet infrastructure they also chill free expression in contravention of Article 10 ECHR.
- d. Fourth, the use by GCHQ of internet and communications service providers' infrastructure to spy on the providers' users on such an enormous scale strikes at the heart of the relationship between those users and the provider

itself. The fact that the internet and communications service providers are essentially deputised by GCHQ to engage in heavily intrusive surveillance of their own customers threatens to damage or destroy the goodwill in that relationship, itself an interference with the provider's rights under A1P1.

7. What is more concerning is that the conduct set out above has no proper justification. Each of the Claimants is a responsible and professional internet service provider. None has any interest in supporting terrorist activity or criminal conduct. They each comply with the law in the countries in which they operate, including UK law in the case of GreenNet, and US law in the case of RiseUp, and to the extent that access is legitimately required to user information held outside the UK, mutual legal assistance arrangements are available.
8. Articles 8, 10, and A1P1 to the Convention each impose requirements as to the nature of the legal justification for any interference. First, they require that the interference be "*in accordance with the law*", "*prescribed by law*", or "*subject to the conditions provided for by law*": in other words that there be a clear and ascertainable legal regime in place which contains sufficient safeguards against abuse of power and arbitrary use. Second, Articles 8 and 10 require that the interference be necessary in a democratic society and a proportionate means of achieving a legitimate aim; A1P1 requires that any deprivation of possessions be "*in the public interest*", which itself imposes a requirement of proportionality.
9. GCHQ has not identified any legal basis for the alleged conduct, which if performed by a private individual would involve the commission of criminal offences. It is assumed at this stage that the justification under domestic law is a warrant issued under s.5 Intelligence Services Act 1994 ("ISA 1994"), which permits "*entry on or interference with property or with wireless telegraphy*" in certain circumstances, and, to the extent that the relevant activities take place outside the British Islands, a warrant under section 7 of the Intelligence Services Act 1994 which purports to immunise from criminal liability "*any act done outside the British Islands, if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section...*".
10. Even if there is such an authorisation under sections 5 or 7 of the 1994 Act, it is nevertheless clear that (i) the interference with Convention rights is not "*in accordance*

with the law", "prescribed by law", or "subject to the conditions provided for by law", since such a warrant may not authorise certain types of CNE under domestic law, there is no adequate public legal regime in place that is capable of meeting those requirements, and (ii) it is not proportionate, both because of the extremely serious nature of the intrusions as against both the internet and communications service providers' employees and their users, and because the activity in pursuit of which the providers' infrastructure is manipulated (mass surveillance, censorship, redirection and modification, and the targeted infection of users' devices) appears to be indiscriminate in nature.

11. These grounds accompany the forms T1 and T2 filed by the Claimants and set out, in summary terms, the grounds relied upon. The Claimants will make detailed submissions and serve evidence in due course, once the Defendants have clarified the nature of their activities and their justification for them.
12. The Claimants also seek a public hearing of their complaint. The fact that documents evidencing the Defendants' activities have been released into and extensively reported on and analysed in the public domain means that there is no longer any good reason to uphold the Defendants' policy of 'neither confirm nor deny' in this case: see *R (Bancoult) v SSFCA* [2013] EWHC 1502 (Admin) at [28] and *CF v SSHD* [2014] EWCA Civ 559 at [20] per Maurice Kay LJ, Sullivan and Briggs LJ agreeing: *"Lurking just below the surface of a case such as this is the governmental policy of "neither confirm nor deny" (NCND)... I do not doubt that there are circumstances in which the courts should respect it. However, it is not a legal principle. Indeed, it is a departure from procedural norms relating to pleading and disclosure. It requires justification similar to the position in relation to public interest immunity (of which it is a form of subset). It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it"*.

THE DEFENDANTS' CONDUCT

13. From June 2013 onwards, a number of public disclosures have been made (beginning with publication in *The Guardian* and *The Washington Post* of documents leaked by a former NSA contractor, Edward Snowden) about programmes of surveillance operated by the NSA with the close involvement of other authorities, including the UK authorities and specifically GCHQ.

14. Many of the revelations concern the scope of the NSA and GCHQ's monitoring of communications, including the "Prism" programme (the monitoring of information stored by telecommunications companies or internet service providers) and "upstream collection" (the direct interception of communications during transmission). Those activities are the subject of existing complaints before the IPT.
15. This complaint relates to more recent revelations regarding GCHQ's intrusion into network infrastructures in order not only to monitor network traffic but also to use the networks to deploy malicious software ("malware") onto individual users' devices.
16. On 20 September 2013, *Der Spiegel* published an article entitled "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm." In that article it wrote:

"Documents from the archive of whistleblower Edward Snowden indicate that Britain's GCHQ intelligence service was behind a cyber attack against Belgacom, a partly state-owned Belgian telecoms company. A "top secret" Government Communications Headquarters (GCHQ) presentation seen by SPIEGEL indicate that the goal of project, conducted under the codename "Operation Socialist," was "to enable better exploitation of Belgacom" and to improve understanding of the provider's infrastructure.

The presentation is undated, but another document indicates that access has been possible since 2010. The document shows that the Belgacom subsidiary Bics, a joint venture between Swisscom and South Africa's MTN, was on the radar of the British spies. [...]

According to the slides in the GCHQ presentation, the attack was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a "Quantum Insert" ("QI"). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware on their computers that can then manipulate them. Some of the employees whose computers were infiltrated had "good access" to important parts of Belgacom's infrastructure, and this seemed to please the British spies, according to the slides.

The documents also suggest that GCHQ continued to probe the areas of infrastructure to which the targeted employees had access. The undated presentation states that they were on the verge of accessing the Belgians' central roaming router. The router is used to process international traffic. According to the presentation, the British wanted to use this access for complex attacks ("Man in the Middle" attacks) on smartphone users. The head of GCHQ's Network Analysis Centre (NAC) described Operation Socialist in the presentation as a 'success.'"

17. Subsequent disclosures, published by *The Intercept* on 12 March 2014, provide further information about the range of network exploitation and intrusion capabilities available to GCHQ. A joint presentation by GCHQ and NSA, entitled "Quantum Theory", depicts the process by which GCHQ exploited network infrastructure for targeted infection of users' devices.⁴ The presentation clarifies that, rather than deploying Man in the Middle attacks, GCHQ and NSA employ a "Man on the Side" technique, which covertly injects data into existing data streams in order to create connections that will enable the targeted infection of users. The technique utilises an automated system - codenamed TURBINE. This system "allow[s] the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually," according to documents released by *The Intercept* on 12 March 2014.⁵ Another undated document claims that TURBINE "will increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants."⁶ Another document, shared with the Five Eyes surveillance alliance (i.e. including GCHQ), referred to TURBINE as permitting "Industrial-scale exploitation."⁷
18. In an article entitled "How the NSA Plans to Infect 'Millions' of Computers with Malware," published on the same date, *The Intercept* details how GCHQ has worked closely with the NSA to develop implants, including "An implant plug-in named CAPTIVATEDAUDIENCE, for example, is used to take over a targeted computer's microphone and record conversations taking place near the device. Another, GUMFISH, can

⁴ <https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/>

⁵ <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>

⁶ <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/>

⁷ <https://firstlook.org/theintercept/document/2014/03/12/industrial-scale-exploitation/>

covertly take over a computer's webcam and snap photographs. FOGGYBOTTOM records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts. GROK is used to log keystrokes. And SALVAGERABBIT exfiltrates data from removable flash drives that connect to an infected computer."

19. In addition to the above, GCHQ has developed extensive means of manipulating mobile devices. The means of compromising such devices, which are invariably internet-enabled, are likely similar if not identical to those of compromising any other computer. Documents published by *The Guardian* on 28 January 2014, in particular a set of slides from a GCHQ presentation delivered on 28 May 2010, revealed that GCHQ had by May 2010 developed a suite of software known as "WARRIOR PRIDE" for iPhones and Android devices, which appeared to allow at least for (i) the activation of a microphone and the taking of recordings without the user's consent ("Hot mic"), (ii) precise identification of the geographical whereabouts of the user ("High precision GEO"), (iii) avoidance of detection that the security of the device has been compromised ("Kernel stealth" and "Self-protection"), and (iv) the retrieval of any content on the phone.

20. In a further article on 11 November 2013 entitled "*GCHQ targets engineers with fake LinkedIn pages*", *Der Spiegel* elaborated on the mechanics of the attack on Belgacom. It described how GCHQ had targeted employees of Belgacom, subjected them to surveillance, and compromised their computers using malware. It also claimed that Belgacom was not the only company that had been targeted in this way.

"The Belgacom employees probably thought nothing was amiss when they pulled up their profiles on LinkedIn, the professional networking site. The pages looked the way they always did, and they didn't take any longer than usual to load.

The victims didn't notice that what they were looking at wasn't the original site but a fake profile with one invisible added feature: a small piece of malware that turned their computers into tools for Britain's GCHQ intelligence service.

The British intelligence workers had already thoroughly researched the engineers. According to a "top secret" GCHQ presentation disclosed by NSA whistleblower Edward Snowden, they began by identifying employees who worked in network

maintenance and security for the partly government-owned Belgian telecommunications company Belgacom. [...]

The computers of these "candidates" were then infected with computer malware that had been placed using infiltration technology the intelligence agency refers to as "Quantum Insert," which enabled the GCHQ spies to deeply infiltrate the Belgacom internal network and that of its subsidiary BICS, which operates a so-called GRX router system. This type of router is required when users make calls or go online with their mobile phones while abroad. [...]

The operation is not an isolated case, but in fact is only one of the signature projects of an elite British Internet intelligence hacking unit working under the auspices of a group called MyNOC, or "My Network Operations Centre." MyNOCs bring together employees from various GCHQ divisions to cooperate on especially tricky operations. In essence, a MyNOC is a unit that specializes in infiltrating foreign networks. [...]

In the case of Mach [a data clearing company which had also been targeted], the GCHQ personnel had "identified three network engineers" to target. Once again, the Quantum Insert method was deployed.

The spies first determine who works for a company identified as a target, using open source data like the LinkedIn professional social networking site. IT personnel and network administrators are apparently of particular interest to the GCHQ attackers, because their computers can provide extensive access privileges to protected corporate infrastructures. [...]

In the case of Mach, for example, the GCHQ spies came across a computer expert working for the company's branch in India. The top-secret document shows how extensively the British intelligence agents investigated the life of the innocent employee, who is listed as a "target" after that.

A complex graph of his digital life depicts the man's name in red crosshairs and lists his work computers and those he uses privately ("suspected tablet PC"). His Skype username is listed, as are his Gmail account and his profile on a social networking site. The British government hackers even gained access to the cookies on the

unsuspecting victim's computers, as well as identifying the IP addresses he uses to surf the web for work or personal use.

In short, GCHQ knew everything about the man's digital life, making him an open book for its spies. [...]

But that was only the preparatory stage. After mapping the man's personal data, now it was time for the attack department to take over. On the basis of this initial information, the spies developed digital attack weapons for six Mach employees, described in the document as "six targeting packs for key individuals," customized for the victims' computers. [...]

Apparently, the agencies use high-speed servers located at key Internet switching points. When a target calls up a specific website, such as LinkedIn, these servers are activated. Instead of the desired website, they supply an exact copy, but one that also smuggles the government hackers' spying code onto the target computers.

According to other secret documents, Quantum is an extremely sophisticated exploitation tool developed by the NSA and comes in various versions. The Quantum Insert method used with Belgacom is especially popular among British and US spies. It was also used by GCHQ to infiltrate the computer network of OPEC's Vienna headquarters. [...]

Much like the Belgacom spying operation, Wylekey is considered a great success. According to a summary, it provided GCHQ with detailed information about Mach, its communications infrastructure, its business profile and various key individuals."

21. A subsequent article published by Der Spiegel on 29 March 2014, "'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel," recounts a similar operation by GCHQ against German infrastructure companies Stellar, Cetel and IABG.

"Stellar operates a satellite ground station in Hürth, a so-called "teleport." Its services are used by companies and institutions; Stellar's customers include Internet providers, telecommunications companies and even a few governments [...] Using their ground stations and leased capacities from satellites, firms like Stellar – or competitors like Cetel in the nearby village of Ruppichterath or IABG, which is

headquartered in Ottobrunn near Munich -- can provide Internet and telephone services in even the most remote areas [...]

The service they offer isn't just attractive to customers who want to improve their connectivity. It is also of interest to Britain's GCHQ intelligence service, which has targeted the German companies. Top secret documents from the archive of NSA whistleblower Edward Snowden viewed by SPIEGEL show that the British spies surveilled employees of several German companies, and have also infiltrated their networks.

One top-secret GCHQ paper claims the agency sought "development of in-depth knowledge of key satellite IP service providers in Germany."

The document, which is undated, states that the goal of the effort was developing wider knowledge of Internet traffic flowing through Germany. The 26-page document explicitly names three of the German companies targeted for surveillance: Stellar, Cetel and IABG.

The operation, carried out at listening stations operated jointly by GCHQ with the NSA in Bude, in Britain's Cornwall region, is largely directed at Internet exchange points used by the ground station to feed the communications of their large customers into the broadband Internet. In addition to spying on the Internet traffic passing through these nodes, the GCHQ workers state they are also seeking to identify important customers of the German teleport providers, their technology suppliers as well as future technical trends in their business sector."

22. Reportedly, GCHQ used similar tactics as with the Belgacom attack, targeting and monitoring employees, particularly engineers, as well as infiltrating and exploiting infrastructure. With respect to IABG, for example, *Der Spiegel* reported that the GCHQ document "includes a list of IABG routers and includes their network addresses. In addition, it contains the email addresses of 16 employees at the company named as possible targets."⁸

23. Another NSA document, shared with GCHQ and published by *The Intercept* on 20 March 2014, describes in further detail how the employees of companies providing

⁸ <http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html>

internet infrastructure services are “hunted” by NSA analysts. Employees performing system administration functions (“sys admins”) are targeted by intelligence agents who, armed with the sys admin’s work email, personal webmail or Facebook credentials can use Quantum to target that individual and subsequently gain access to the internet and communications service provider’s entire network. In a post to an internal NSA forum entitled “*I hunt sys admins*”, one agent describes the process as follows:

*“Up front, sys admins generally are not my end target. My end target is the extremist/terrorist or government official that happens to be using the network some admin takes care of. Sys admins are a means to an end. For example, assume your target is using a CDMA device [i.e. a mobile telephone] on a foreign network: there may be situations where we passively collect his phone call/SMS out in the wild, but it would be ***really*** nice if we had access to the local infrastructure where we could monitor which tower he’s connected to at any given point in time, or monitor all phone calls/data traffic that his phone generates. Many times, its difficult to directly target infrastructure... generally we’ll need a fair amount of information going into an operation [...] In order to get that, who better to target the person that already has the ‘keys to the kingdom’? Many times, as soon as I see a target show up on a new network, one of my first goals is, “Can we get CNE access to the admins on that network, in order to get access to the infrastructure that target is using?”*

24. An excerpt from a further NSA document, published by *The Intercept* on 12 March 2014 makes the same point under the description “hacking routers”.⁹ The author writes:

“[...] let’s go over some of the things that someone could do if they hack a router:

- *You could add credentials, allowing yourself to log in any time you choose*
- *You could add/change routing rules*
- *You could set up a packet capture capability... imagine running Wireshark on an ISP’s infrastructure router... like a local listening post for any credentials being passed over the wire(!)*

⁹ <https://firstlook.org/theintercept/document/2014/03/12/five-eyes-hacking-large-routers/>

- *You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels[...]*"

The author concludes: *"Hacking routers has been good business for us and our 5-eyes partners for some time now [...]"*.

25. It is not known (not least because there is no clear or accessible legal regime governing it) how many such attacks have been carried out, against whom, what damage has been caused to the targeted internet and communications service providers' systems, how many providers' employees have been specifically targeted and subjected to surveillance, how many users subjected to mass and intrusive surveillance and users' devices compromised as a result, who has access to the information collected as a result of all the above, for how long and on what terms. That is itself a significant cause for concern. But in any event there are two other concerns as a matter of principle.

- a. First, the process of exploiting an internet and communications service provider's infrastructure obviously involves a breaching the security of the infrastructure. It is therefore highly likely that any such breach compromises the security of the network going forward, leaving the infrastructure open to further damage or exploitation by a third party. For instance, the changes necessary to compromise the system may result in security vulnerabilities that could be exploited by third parties in other ways. As well as simply being a byproduct of compromising the network, the weakening of security may even be deliberate, as the reference in the document quoted at paragraph 24 above to *"weaken[ing] any VPN encryption capabilities on the router"* makes clear.
- b. Second, the tools allow GCHQ access to a large amount of highly private data pertaining to both an internet and communications service provider's employees and its users, including all individuals whose communications may pass through the internet and communications service provider's infrastructure. That is not only relevant to the level and proportionality of the interference with the rights of the internet and communications service providers' employees and users; it is also relevant to the impact on the internet and communications service providers' business due to the fact that

their systems are being used as a means of facilitating extremely intrusive surveillance of their own customers. On any view, GCHQ's interferences are of unprecedented scope and seriousness:

- i. The information stored on a computer or mobile device is potentially far more comprehensive than the information that an individual communicates over a network in a manner capable of interception, or even information that could be obtained from a search of his home or office. These devices may contain not only details about the user's personal circumstances (for instance his age, gender, or sexual orientation), but also financial information, unencrypted passwords, privileged legal information and so on. Unlike in the case of an interception of communications, even information that the user deems too personal, private or sensitive to communicate is vulnerable to collection or monitoring when intrusion tools are utilised.
- ii. Moreover, GCHQ's intrusive malware also appears to grant total control over the device, enabling the manipulation of functions including the camera and microphone without authorisation, and thereby the gathering of data which the user has never even chosen to store, let alone communicate to others.
- iii. Finally, the intrusion is compounded by (a) the fact that, unlike in the case of a lawful search of a home or office, the user has little or no way of knowing that it has happened, and (b) compromised devices are likely to be left more vulnerable by virtue of the breaches necessary to enable the installation of the malware.

26. Further, there have been clear indications that GCHQ itself has reservations about the legality of such operations.

- a. An undated NSA document referring to a trilateral programme between "NSA, GCHQ, and FRA" (the Swedish signals intelligence agency) for the deployment of the Quantum technique says: "*Continued GCHQ involvement*

may be in jeopardy due to British legal/policy restrictions".¹⁰ There is no further explanation of the concerns.

- b. A document prepared by a representative of GCHQ for an international telecommunications conference in September 2010 reads, in relation to the implanting of software to decrypt communications encrypted with a particular standard ("MIKEY-IBAKE"): *"An additional concern in the UK is that performing an active attack, such as the Man-in-the-Middle attack proposed in the Lawful Interception solution for MIKEY-IBAKE may be illegal. The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material. A Man-in-the-Middle attack causes modification to computer data and will impact the reliability of the data. As a result, it is likely that LEMFs and PLMNs would be unable to perform LI on MIKEY-IBAKE within the current legal constraints."*

Effect on the Claimants

27. In order to pursue this complaint, the Claimants need not show that they or their employees have actually been the subject of the alleged interference.

- a. In the context of monitoring of communications, the European Court of Human Rights has held that *"the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under art.8, irrespective of any measures actually taken against them"*: Liberty v United Kingdom (2009) 48 EHRR 1 at [56].
- b. For the reasons given above, the interference in the present case is more serious than the monitoring of communications: it is the active manipulation

¹⁰ <https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html>

of the internet and communications service provider's property, its employees and its users so as to enable the collection of data, including data which has never been communicated. Accordingly, the same principle applies in this case.

c. Likewise, if "*the mere existence of legislation*" permitting interference is a sufficient interference with a fundamental freedom to justify a legal challenge, then the fact that there is evidence of an interference without any meaningful legislative control is an even clearer case where a complainant need not show actual interference with his own affairs. In those circumstances, where there is no statutory scheme, Code of Practice or published policy indicating who can be targeted and in what circumstances, it is even more difficult for an individual to know whether they have been subject to the relevant activity.

d. Similarly, in the specific case of A1P1 and the effect on the internet and communications service providers' business dealings with their consumers, the very fact that there is an unconstrained prospect of the internet and communications service provider's network being used as a means of highly intrusive surveillance of its users damages the goodwill between the two, even if that surveillance is not in fact carried out.

28. The Claimants are clearly within the category of persons who may be affected by the interference; they, like Belgacom and the other companies known to have been affected, are providers of internet and communications services. Accordingly, the interference (i) affects the employees' personal data and impairs their freedom to communicate, (ii) in doing so, prevents the internet and communications service providers themselves from imparting and receiving information freely, and (iii) independently of that interference, it jeopardises the provider's relationships with its customers and potentially damages its property.

29. In fact, the Claimants are particularly susceptible to the A1P1 interference that will arise from destruction of or damage to customer goodwill, in that their brand profile is based to some extent a core belief in fundamental human rights and respect for the rule of law: their customer bases therefore consist in substantial part of individuals and organisations who have relied on those shared values to ensure their

communications are protected, and who are likely to be particularly concerned about mass and intrusive surveillance.

- a. GreenNet advertises itself as *"the ethical Internet Service Provider that has been connecting people and groups who work for peace, the environment, gender equality and human rights since 1986"*.
- b. RiseUp advertises itself as providing *"online communication tools for people and groups working on liberatory social change. We are a project to create democratic alternatives and practice self-determination by controlling our own secure means of communications."*
- c. Jinbonet, the Korean Progressive Network, is described by the Association for Progressive Communications as an organisation that *"aims to support the growth of civil activity and communication by providing network services such as web hosting, community, e-mail, blog, progressive meta blog, mailinglist, etc to civil society organizations, trade unions, individuals and progressive projects."*
- d. Greenhost advertises itself as offering *"a fresh approach to ICT and sustainability, and also supports various projects in the fields of education, culture and journalism. We are committed to a free and open internet and the security of our users."*
- e. May First/People Link describes itself as *"a politically progressive member-run and controlled organization that redefines the concept of "Internet Service Provider" in a collective and collaborative way,"* and notes that its members are *"organizers and activists."*
- f. Chaos Computer Club describes itself as a non-profit association with 3,600 members which *"[f]or more than thirty years [has been] providing information about technical and societal issues, such as surveillance, privacy, freedom of information, hactivism, [and] data security."*

LEGAL FRAMEWORK

Human Rights Act 1998 and European Convention of Human Rights

30. By s.6 Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates various rights from the European Convention including Articles 8 and 10 and A1P1.

31. Article 8 of the Convention provides:

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

32. Article 10 provides:

1. *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

33. Article 1 of the First Protocol provides:

“Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public

interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties."

34. The concept of 'possessions' in A1P1 covers all forms of property, including those which the applicant has only a legitimate expectation of receiving (*Kopecky v Slovakia* (2005) 41 EHRR 43). It has been held to include the goodwill or economic interests connected with the running of a business (*Tre Traktorier Aktiebolag v Sweden* (1989) 13 EHRR 309).
35. In *Hutten-Czapska v Poland* (2006) 42 EHRR 15 at 167-168, the Grand Chamber restated the principles governing justification of an interference with A1P1:

"Not only must an interference with the right of property pursue, on the facts as well as in principle, a 'legitimate aim' in the 'general interest', but there must also be a reasonable relationship of proportionality between the means employed and the aim sought to be realised by any measures applied by the state, including measures designed to control the use of the individual's property. That requirement is expressed by the notion of a 'fair balance' that must be struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights. The concern to achieve this balance is reflected in the structure of article 1 of Protocol No 1 as a whole. In each case involving an alleged violation of that article the court must therefore ascertain whether by reason of the State's interference the person concerned had to bear a disproportionate and excessive burden. [...] In cases concerning the operation of wide-ranging housing legislation, that assessment may involve not only the conditions for reducing the rent received by individual landlords and the extent of the State's interference with freedom of contract and contractual relations in the lease market but also the existence of procedural and other safeguards ensuring that the operation of the system and its impact on a landlord's property rights are neither arbitrary nor unforeseeable. Uncertainty - be it legislative, administrative or arising from practices applied by the authorities - is a factor to be taken into account in assessing the State's conduct."

36. There are therefore four questions in any analysis of whether those rights have been breached:

- a. Is the relevant right engaged?
- b. Does the interference comply with the requirement of legal certainty imposed by the relevant Article?
- c. Is the interference in pursuit of a legitimate aim?
- d. Is the interference proportionate to the goal which is sought to be achieved (and, in the case of Articles 8 and 10, “*necessary in a democratic society*”)?

Engagement of rights

37. Each of the rights is clearly engaged in the present case.

- a. As for Article 8, it is clear from the documents revealed by *Der Spiegel* that the employees targeted in the attack on Belgacom were subjected to deep personal surveillance. Even the GCHQ presentation (which appears to have been used for training purposes, and therefore with most of the relevant GCHQ staff having absolutely no need to know his personal information) made reference to an individual’s name, a list of the computers he used at work and privately, his Skype username, his Gmail account, a social networking profile belonging to him, his IP addresses and the cookies on his computers (As *Der Spiegel* reported: “*In short, GCHQ knew everything about the man’s digital life*”). This information appears to have been widely disseminated within GCHQ. All of those things are obviously private information within the meaning of Article 8. By way of example, the European Court of Human Rights has held in the context of workplace monitoring that that “*emails sent from work*” and “*information derived from the monitoring of personal internet usage*” are both protected by Article 8: *Copland v United Kingdom* (2007) 45 EHRR 37 at [41].
- b. The Article 8 rights of the internet and communications service providers’ users are also affected by GCHQ’s conduct. Exploitation of the internet and communications service providers’ infrastructure enables GCHQ to conduct

surveillance on users of the providers' services, either through mass monitoring or filtering of communications, or through the targeted infection of users' devices with malware.

- c. As for Article 10, the Court has recognised in *Weber* (above, [144-145]) that the fact that "the threat of secret surveillance [...] necessarily strikes at the freedom of communication of users of telecommunications services" means that it engages Article 10 if the effect is to discourage communications. The same principle must apply to the threat of intrusion into computers and devices via the internet, to the extent that it discourages the free use of the internet, which it obviously will if left uncontrolled.
- d. As for A1P1, (i) to the extent that the internet and communications service providers' computers and network assets have been damaged or materially altered in the course of such an attack there will obviously be an interference with its property, and (ii) in any event, the unauthorised deputisation of the internet and communications service provider to assist GCHQ in spying on its customers will have an obviously detrimental effect on the provider's commercial relationships and the goodwill it enjoys, which is a 'possession' within the meaning of A1P1 as set out above.

Legal certainty

38. It is well settled that the requirements set out in Articles 8 and 10, that the interference be "in accordance with the law" or "prescribed by law", demand more than merely that the interference be lawful as a matter of English law: it must also be "compatible with the rule of law": *Gillan v United Kingdom* (2010) 50 EHRR 45 at [76]. That means it must "afford a measure of legal protection against arbitrary interferences by public authorities", and indicate "with sufficient clarity" the scope of any discretion conferred and the manner of its exercise: *Gillan* at [77].
39. Although the text of A1P1 only provides expressly that any deprivation of possessions must be "subject to the conditions provided for by law", the same principle applies equally to interferences with possessions. In *Amat-G Ltd v Georgia* (2007) EHRR 35, the ECtHR held at [58-61] that an interference which was neither a deprivation nor a control of use could nevertheless only be lawful if it "satisfied the

requirement of lawfulness and was not arbitrary”, stating that “the rule of law, one of the fundamental principles of a democratic society, is inherent in all provisions of the Convention”. The three Articles may therefore be treated as identical for the purposes of this criterion.

40. Numerous cases have addressed this requirement in the context of secret surveillance and information gathering.

- a. In *Malone v United Kingdom* (1985) 7 EHRR 14, the Court held that the legal regime governing interception of communications “must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence” [67]. It must be clear “what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive” and the law must indicate “with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities” [79].
- b. In *Association for European Integration and Human Rights v Bulgaria* (62540/00, 28 June 2007), the Court held at [75]: “In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated [...]”.
- c. These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the “procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material” (*Liberty v UK* (2009) 48 EHRR 1 at [69]).
- d. In *Weber* the ECHR held at [93-94]: “The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures [...] Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion

granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.”

- e. The Court continued in *Weber* by setting out the matters which any legal regime governing secret surveillance must expressly address in statute in order to be regarded as lawful:

95 In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.

Legitimate aim and proportionality

41. The Claimants accept that, in principle, surveillance may be conducted for legitimate aims such as national security. As set out in more detail below, they deny that the interference in this case is a proportionate means of achieving such a legitimate aim.

Domestic legal regime governing the relevant conduct

Regulation of Investigatory Powers Act 2000

42. RIPA 2000 regulates, among other things, the interception of communications in the course of transmission (Part I Chapter I), the acquisition of communication data from persons providing a telecommunication service (Part I Chapter II), and intrusive surveillance and covert human intelligence sources (Part II), in the UK.
43. Part I Chapter I empowers the Secretary of State to issue warrants for the interception of communications under s.5, if he considers the interception necessary

on a number of listed grounds, including national security, and proportionate to the aim to be achieved.

44. Section 2(2) RIPA 2000 defines “interception” as follows:

“a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he –

(a) so modifies or interferes with the system, or its operation,

(b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.”

45. That might extend to some of the effects of the conduct at issue in this complaint – for instance, if malware were implanted and then used in order to record a phone call while it is being made – but it does not cover most of the functions described in the leaked documents. For example, the extraction of documents from a hard disk or a mobile device would not be the interception of a communication in the course of its transmission; it might involve the collection by GCHQ of information which the affected individual never intended to share with anyone. Likewise, the ability to activate a user’s camera or microphone without his knowledge would not involve the interception of any communication. Accordingly, it cannot be said that the implanting of malware is merely a modification “so [...] as to make some or all of the contents of the communication available while being transmitted”.

46. RIPA Part I Chapter II covers the acquisition and disclosure of “communication data”, namely data held by a person providing a telecommunication service (section 21(4)). That is clearly not engaged.

47. Part II is not engaged either; s.48(3) provides that “References in this Part to surveillance do not include references to [...] (c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under – (i) section 5 of the

Intelligence Services Act 1994 [...]. In a case involving interference with property by GCHQ, which (as set out below) is governed by the Intelligence Services Act 1994, that exemption applies. In any event, nowhere in Part II is there any reference to the manipulation of electronic devices belonging to others; the Act is clearly aimed at a different kind of information-gathering, its interpretation provisions referring to "monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications", either by officials alone or "by or with the assistance of a surveillance device" (s.48(2)), and only in certain circumstances "the interception of a communication in the course of its transmission". As an interference with fundamental rights it cannot lightly be construed as covering an entirely different kind of information-gathering: *R (Simms) v SSHD* [2000] 2 AC 115. In any event, it does not even arguably extend to activity such as the collection and extraction of documents.

Computer Misuse Act 1990

48. It is an offence under s.1(1) Computer Misuse Act 1990 ("CMA 1990") to cause a computer to perform any function with intent to secure access to any program or data held in it, or to enable any such access to be secured, if the access is unauthorised and known to be unauthorised. (The term "computer" is not defined in the Act, but in another statutory context was held by Lord Hoffmann in *DPP v McKeown* [1997] 1 WLR 295 to mean "a device for storing, processing and retrieving information". Modern mobile devices, which are far more sophisticated and powerful than the desktop computers available when the Act was passed, undoubtedly qualify.)
49. Further, under s.3 CMA 1990 it is an offence to do any unauthorised act in relation to a computer, in the knowledge that it is unauthorised, if (i) the intention is to impair the operation of the computer, to prevent or hinder access to any program or data, to impair the operation of any program or the reliability of any data, or to enable any of those things, or (ii) the perpetrator is reckless as to whether the act will do any of those things. S.3(5) clarifies that the relevant effects may be only temporary, and also that a reference to doing an act includes a reference to causing an act to be done. The result is that the infection of a computer pursuant to an automated process would still be an offence on the part of the person who commenced or directed that process. The intrusion at issue here not only impairs the operation of the target computers in

multiple ways, including by draining battery life and using bandwidth and other computer resources, undermining security features such as encryption and intrusion prevention. The intrusion also impairs the actual network infrastructure owned and operated by the internet and communications service providers, and the services and programs run on the infrastructure.

50. S.10 CMA 1990 provides that section 1(1) *"has effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and (b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure."* However, this override does not apply to section 3(1). Therefore, at least to the extent that such activities occur in England and Wales, any GCHQ activities that impair the operation of a computer - for instance, by leaving it vulnerable to future exploitation, as explained above are *prima facie* unlawful.

Intelligence Services Act 1994

51. S.3 ISA 1994 provides the statutory basis for GCHQ and delineates its statutory functions. Those functions include *"to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide [to various organisations] information derived from or related to such emissions or equipment and from encrypted material"*. By s.3(2) those functions are exercisable only in the interests of national security, the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands, or in support of the prevention or detection of serious crime.
52. S.4(2) requires the Director of GCHQ to ensure *"that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings."*
53. S.5(1) provides: *"No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section."* The Secretary of State may issue such a warrant on the application of GCHQ in respect of any action, provided he *"thinks it necessary for the action to be taken for the purpose of assisting [...] GCHQ in carrying out [its statutory functions]," "is satisfied that the taking of the action is proportionate to what the action seeks to achieve"*, and is satisfied

that satisfactory arrangements are in force with respect to section 4(2) in relation to onward disclosure.

54. In other words, the apparent legal basis for the activity at issue in this complaint is an extremely broad power on the part of the Secretary of State to render lawful what would otherwise be unlawful.

GROUND 1: IN ACCORDANCE WITH LAW/PREScribed BY LAW

55. As already indicated, there are three types of activity at issue in this complaint. The first relates to the manipulation of the targeted internet and communications service providers' property and the unauthorised changes made to its assets and infrastructure. The second and third relate to the surveillance of the internet and communications service providers' employees and customers respectively.

56. Together they form part of a covert and potentially enormous programme of surveillance which has only come to light as a result of unauthorised disclosures. The nature of that programme of surveillance, under which internet and communications service providers, their employees or their customers may have no idea they have even been subjected to it, is such that it cannot possibly be Convention-compliant in the absence of a clear legal framework governing its use.

- a. The surveillance which it is aimed at facilitating has the potential to be more intrusive than any other form of surveillance or data-gathering. The amount of information stored on mobile phones and computers is vast, and much of it will be highly personal in nature. Unlike the monitoring of communications, these activities enable GCHQ to obtain that information whether or not the affected individual has ever chosen to share it with anyone.
- b. Moreover, the logging of keystrokes and the covert activation of cameras and microphones enable GCHQ to obtain further potentially sensitive information whether or not the affected individual has ever chosen even to store it.
- c. A user may not even know of the full extent of what his computers or mobile devices store. A mobile phone may, for instance, log all his historical

geographical movements as well as his current location. For instance, if he went for a job interview or a medical appointment during work hours, that would be logged regardless of whether there were any other record of that interview or appointment having been arranged.

- d. The fact that computers and devices are vulnerable to intrusion in this way will inevitably discourage people from using the internet freely.
 - e. The potential vulnerabilities resulting from the forcible infection of devices and the necessary weakening of security that such manipulation involves have the potential to produce further interferences beyond those which GCHQ directly controls.
 - f. The potential for GCHQ to take over a compromised device altogether, potentially altering its contents, raises serious concerns about the integrity of any evidence from such sources that might be used in legal proceedings, and the mechanisms would should be established and enforced in order to ensure that that integrity is protected.
 - g. As a matter of general principle, the fact that computer hacking involves sophisticated technology and concepts which were unknown 20 years ago strongly militates in favour of a requirement that it be governed by an appropriate legal framework developed with that technology and those concepts in mind.
57. Accordingly, it is if anything more necessary than in an ordinary 'interception' case that there be a clear legal framework governing activities of this sort.
58. There is no such framework. The only statutory scheme dealing expressly with the unauthorised infection of computers was established in 1990. Far from establishing a Convention-compliant framework within which such infection is to be permissible on certain conditions and with certain safeguards, it makes clear that GCHQ's activity is simply unlawful in the absence of a supervening provision. The availability of a warrant under ISA 1994 that simply cancels any unlawfulness is self-evidently not an adequate safeguard.

59. There is no Code of Practice governing the circumstances in which intrusion will be permitted, by what means, against whom, in response to what level of suspicion and for what kind of misconduct, or for how long their systems will be permitted to remain compromised. Nor is there anything governing the procedure to be followed in selecting for examination, sharing, storing and destroying any material obtained (*Liberty* at [69]), or anything governing the relationship between GCHQ's programme and the equivalent programmes being pursued by the NSA, FRA, and potentially others. Even if it is strictly speaking permissible as a matter of construction of domestic law (which, given the Defendants have not yet advanced any such case, is not admitted), it falls short of the requirements of the rule of law and of the various articles of the Convention which import those requirements.

GROUND 2: DISPROPORTIONALITY OF INTERFERENCE

60. Given the limited availability of the details of GCHQ's activity (still less the purported legal basis for it) to the Claimants at this stage, the Claimants must reserve the right to make more detailed submissions on the disproportionality of the interference in due course.

61. For present purposes it is sufficient to say:

- a. As set out above, the nature of the intrusion carried out against internet and communications service providers' employees and customers is far more serious than the interception of their communications and, if left unchecked, amounts to one of the most intrusive forms of surveillance any government has ever conducted. The amount of data which can be collected, and the speed, ease and surreptitiousness with which it can be done, is completely unprecedented. In those circumstances any such intrusion would have to be highly targeted and justified by very specific circumstances in order for the activity to be proportionate to any legitimate aim.
- b. All the indications so far are that the activity goes far beyond any such specific justification. Indeed, the compromising of network infrastructures would tend to suggest the opposite: as reported by *The Intercept* in March 2014, the NSA (with the cooperation of GCHQ) intends to use those infrastructures to deploy malware into "millions" of devices.

- c. Moreover, the lack of safeguards mentioned above – in particular the apparent lack of any restriction on the extent or duration of the infection of any particular device – tends strongly against any finding that the interference is proportionate to any legitimate aim.
- d. There is nothing in the publicly available documents relating to the attack on Belgacom which suggests that there was any specific justification for targeting Belgacom in particular, other than the fact that it was an operator of major network infrastructure and that this would enable the infection of its users' devices.

CONCLUSION

- 62. The Claimants therefore seek the following orders (which, again, may have to be supplemented or amended in light of further disclosures):
 - a. A declaration that GCHQ's intrusion into the computers and network assets of internet and communications service providers, their staff and their users is unlawful and contrary to Articles 8 and 10 and A1P1 ECHR;
 - b. An order requiring the destruction of any unlawfully obtained material;
 - c. An injunction restraining further unlawful conduct.
- 63. The Claimants adopt and support, mutatis mutandis, the amendments and re-amendments made in the *Privacy International* claim.

Ben Jaffey
Tom Cleaver
Blackstone Chambers

July 2014
Ben Jaffey
Tom Cleaver
Blackstone Chambers

19 May 2015
13 July 2015

○

○

IN THE INVESTIGATORY POWERS TRIBUNAL

Case No. IPT 14/85/CH

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL

Case No. IPT 14/120-126/CH

BETWEEN:

GREENNET LIMITED

RISEUP NETWORKS, INC

MANGO EMAIL SERVICE

KOREAN PROGRESSIVE NETWORK ("JINBONET")

GREENHOST

MEDIA JUMPSTART, INC

CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

Expert report of Professor Ross Anderson

I, Ross John Anderson, will say as follows.

1. I am Professor of Security Engineering at Cambridge University where I have been a member of faculty at the Computer Laboratory since 1995. I am a Fellow of the Royal Society and the Royal Academy of Engineering, and have won the Lovelace Medal, the top UK award in computing. I am also an elected member of Council, the University's executive body.
2. I have worked or consulted for a wide range of technology companies both before joining Cambridge and since, including IBM, Microsoft, Intel, Google and Samsung. I have also consulted for financial services and utility firms from Standard Chartered Bank to the Electricity Supply Commission of South Africa. I have over thirty years' experience working with computer and communications security, including cryptography, in both industry and academia. My CV can be downloaded from my web page¹.
3. Since coming to Cambridge in 1992 I have made pioneering contributions to a number of new areas of research and practice, including the economics of information security, crypto protocols, API security, digital copyright marking and hardware tamper-resistance.
4. The grand challenge tackled by my research is developing the discipline of security engineering: building systems to remain dependable in the face of malice, error or mischance. This focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves. Security engineering is inherently multidisciplinary, as the hard problems in a globalised world usually have interlinked challenges in engineering, psychology, and economics.
5. This report is chiefly concerned with items 5 and 6 (d)-(f) in the Proposed Legal Issues and the consequences of seeking or inducing weaknesses in security facilities. By using computer and network exploitation (CNE) to obtain easier access to information, GCHQ and its partner agencies often inflict very substantial harm on others and indeed on the economy as a whole by weakening the essential electronic infrastructure upon which the world's economy and stability depends. This 'equities issue' is already recognised in US policy and a number of senior former intelligence community officials now acknowledge that the NSA and FBI got the balance wrong in the past². UK policy and oversight need to be reconsidered accordingly.

¹ See <http://www.ross-anderson.com> or <http://www.cl.cam.ac.uk/~rja14>

² "Obama administration explored ways to bypass smartphone encryption", Andrea Peterson and

² "Obama administration explored ways to bypass smartphone encryption", Andrea Peterson and Ellen Nakashima, Washington Post, Sep 24, at https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-see-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html

Scope

6. Security engineering is not just about protecting 'computers' from hacking but about the large and growing number of systems that rely on computation, communication or both. Examples include card payment systems, prepayment electricity meters, burglar alarms, goods vehicle tachographs and speed limiters, taximeters and vending machines³. (I have been engaged in research and/or development work on all of these.) New systems coming onstream now or in the near future include implantable medical devices, remotely piloted aircraft and self-driving cars.
7. Every single one of these devices is of active or potential interest to law enforcement and intelligence agencies, and every single one uses cryptography, access control mechanisms, or both – the same mechanisms used to protect email and e-commerce against snoopers and hackers.
8. Thus when we talk about law-enforcement access to systems we are not merely discussing who can read your email. Who can read your electricity meter? (The drugs squad would like to know who's running a lot of lamps.) Who can defeat your burglar alarm? (Perhaps the covert-entry teams at MI5 would value that.) And can a police officer stop your car other than by stepping in front of you and raising his arm? (There are discussions on technical standards for doing just that with autonomous vehicles and indeed even for vehicles controlled by human drivers⁴.)
9. Starting in the 1970s with the invention of the microprocessor, computers have been finding their way into more and more devices. In the 1990s these were called 'embedded systems'; in the 2000s 'things that think'; nowadays it's 'the Internet of Things'. More and more devices contain software, and communicate with online services.
10. Online communications can be a lifesaver. Many modern cars will alert a central reporting centre if the airbags deploy. Many have an emergency call button with which the driver can summon help after an accident. There is no need for people injured in a car crash to die slowly at the side of the road because no-one called 999 for an ambulance⁵.
11. Even toy dolls now talk to data centres. Kids love toys that respond to their voices, but doing voice-recognition in the toy itself would cut the battery life to days or even hours. The solution is to send the child's speech over the home wifi to a remote data centre

³ See my textbook "Security Engineering", RJ Anderson, Wiley 2008; also available free online at <http://www.cl.cam.ac.uk/~rja14/book.html>

⁴ "EU has secret plan for police to 'remote stop' cars", Bruno Waterfield and Matthew Day, Daily Telegraph 29 Jan 2014

⁵ "Lamara Bell dies of injuries sustained in M9 car crash", Libby Brooks, The Guardian, 12 July 2015

where it can be understood and commands send back to the toy⁶. Gesture interfaces are also spreading, and the video-recognition tasks involved are even more computationally intensive and thus even more likely to be done remotely.

12. A 2014 report by the US President's Council of Advisers on Science and Technology predicted that because of the spread of voice and gesture interfaces, almost every inhabited space on the planet will soon have in it microphones and cameras that are connected to data centres, many of them in everyday devices⁷.
13. It will become increasingly common for the software in everyday devices, like the software in a PC or phone, to be updated remotely by the vendor or service provider. This enables businesses to add features and marketing offers. In the case of safety-critical products such as cars it will let some problems be fixed remotely, avoiding the cost of physical recalls, and making it feasible to fix more problems. It will also be ever more important to fix such security vulnerabilities as are discovered from time to time.
14. Thus when we discuss computer and network exploitation (CNE) for the purposes of intrusive surveillance we are not just talking about objects that are recognisably a 'computer'. Many other devices can also be pressed into service.
15. A law enforcement or intelligence agent wishing to place a crime boss under surveillance could also somehow access the microphone in his child's toy, or the server in the data centre that turns the speech into text and thus into commands to the toy.
16. A drugs gang that always deals heroin in the back of a moving taxi could be placed under surveillance by a traditional radio microphone, inserted physically under the seat; alternatively, agents could hack the dealer's mobile phone and turn on the microphone; and if the dealer leaves his phone at home, agents could hack the car and turn on the microphone used for voice commands, or even the microphone provided to make emergency calls.
17. Successive FBI chiefs have complained that the world is 'going dark' because of encryption⁸. The reality is that although some service providers turn on encryption (often to stop competitors stealing their ads), the spread of computers and communications has created a cornucopia of new sources for law enforcement and intelligence. It used to cost thousands of pounds a day to follow a suspect around; now, mobile phone location traces

⁶ "Privacy advocates try to keep 'creepy,' 'eavesdropping' Hello Barbie from hitting shelves", Sarah Halzack, Washington Post, 11 March 2015

⁷ "Report to the President – Big Data and Privacy: A Technological Perspective", President's Council of Advisers on Science and Technology, May 2014

⁸ See for example Director James B. Comey at Brookings Institute, 16 October 2015; text at <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>

are easily available. And while people used to do business on the phone or in person, now people use email, text and chat. Material that would only be recorded if someone took the trouble is now archived automatically and is potentially available as evidence unless every single recipient takes the trouble to delete it, and does so competently.

The costs and risks of CNE

18. It is against this background that the Tribunal should consider the proper regulation of computer and network exploitation (CNE) for law enforcement and intelligence purposes. Where the 'Proposed Legal Issues' document refers to a 'device', it can mean not just a smartphone, but also your car, your electricity meter, your child's toy doll or even the laboratory equipment being used to analyse your blood test in a hospital. The same goes for the Home Office's Draft Equipment Interference Code of Practice.
19. I first consider the use of CNE by a law enforcement agency against a named individual target when they have a warrant to do so. The targeted surveillance of someone against whom an investigator has shown probable cause, or reasonable suspicion (depending on the jurisdiction), to an independent party who has assessed whether the intrusion is proportionate and necessary, is a reasonable extension of how civilised societies have dealt with law enforcement intrusion into physical property for many years.
20. Targeted CNE does however face several challenges. First, the intrusion may render any information collected difficult or impossible to use in evidence; the target, or some other criminal defendant, might claim that any evidence claimed to be found on his computer had been put there by the police. Whether such a claim is true or not in any particular cases, its possibility has consequences. My colleague Professor Peter Sommer, who has extensive experience in computer evidence, will discuss them in a separate report.
21. Second, the intrusion may place lives at risk. For example, in one of the first distributed denial-of-service attacks, an ISP (Panix in New York) had its service taken down by political opponents who hacked a number of servers in hospitals in Oregon and installed malware on them. These servers then bombarded Panix with traffic, depriving its customers of Internet service⁹. The hospital servers were easy targets because their FDA certification required them to be kept in an insecure state; they could not be upgraded with security patches as this would have voided their safety approval. Interference by hackers with medical equipment carries clear and present risks.
22. No harm to patients was reported in the Panix case, and while patients have been killed by software failures in a number of other reported cases, we do not yet have any documented incidents of people being killed by hacking attacks against machines on

⁹ "Distributed Denial of Service Attacks", Charalampos Patrikakis, *The Internet Protocol Journal* Volume 7, Number 4

which they depended. (Hacking attacks have cost lives in other contexts; see for example the two suicides reported by the police in Canada following the Ashley Madison hack¹⁰.)

23. Nonetheless, in my opinion it is only a matter of time before CNE causes fatal accidents. Computers are becoming embedded in ever more devices, on which human societies depend ever more in ways that are complex and ever harder to predict.
24. In addition to safety hazards, CNE carries political risks that have been underestimated in the past. A recent example is the disclosure that GCHQ hacked Belgacom in order to conduct surveillance of EU institutions¹¹. Given that much of the UK's law is made there, this is almost as if the First Minister of Scotland had authorised Police Scotland to conduct surveillance of Whitehall by hacking BT. The Tribunal might ponder whether such an operation would have ever taken place if it had required specific authorisation, whether from a minister or a judge.
25. For this reason, security experts are overwhelmingly opposed to the use of CNE on a vigilante basis even in those jurisdictions where it is still legal. It is simply not safe to "hack back", as the machine that is being used to attack you and which you want taken offline might be providing a safety-critical service somewhere, or might belong to an institution with some kind of power or authority that could harm you.
26. Yet despite the hazards of hacking unknown devices, criminals routinely do so, mainly in order to assemble botnets – collections of compromised machines under their command and control which they use to perform criminal tasks, such as sending phishing emails (emails that purport to be from your bank and invite you to enter your bank credentials at a fake website) and mounting denial-of-service attacks.
27. We analysed the costs to the UK and global economy in a 2013 report commissioned by the Chief Scientific Adviser at the Ministry of Defence. While some specific cyber crimes can be costed separately, an ever-larger part of the direct cost of cybercrime relates to the shared infrastructure created to support crime – most notably the 'botnets' or networks of infected computers which criminals create in order to send spam, conduct phishing attacks against bank credentials, launch distributed denial-of-service attacks for hire or for ransom, and even host unlawful content. The global direct costs are estimated to be of the order of \$4–5bn while the indirect costs – the time and effort taken to clean up infected machines – is estimated at \$10bn for companies and the same again for individuals. The broader social costs to the global economy include a further \$10bn to individuals of economic activity avoided because of fear of cybercrime, while the cost to merchants of people being reluctant to shop online because of security concerns is double

¹⁰ "Toronto police report two suicides associated with Ashley Madison hack", Sam Thielman, *The Guardian*, 24 August 2015

¹¹ "Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm", *Der Spiegel*, 20 September 2013

that again¹². Because of the difficulties in measuring the costs of crime, these must be seen as no more than defensible order-of-magnitude estimates. However it is notable that an earlier Cabinet Office report estimated the direct and indirect costs of cybercrime to the UK economy at about double the figures in the 2013 report¹³.

Use of CNE by nation states and their proxies

28. There have been many news stories of large-scale attacks on networks and computers that caused significant disruption, including attacks on civilian infrastructure in Estonia and Georgia after these countries had disputes with Russia. These attacks were said by some to be the work of the Russian state but ascribed by others ethnic Russian hackers¹⁴. There were also some very damaging attacks on Sony that were said by the US government to be the work of North Korean state agents¹⁵.
29. My own group has direct experience of an attack from China on the private office of the Dalai Lama in 2008 at the time of the Beijing Olympics. We received a call for help from the Tibetan government in exile and I sent an Indian research student, who happened to be in Delhi at the time, up to Dharamsala to help. We discovered that perhaps 35 of the 50 PCs in the Tibetan leader's office had been compromised and information was being sent to three locations in China associated with military and intelligence units tasked with different aspects of Tibet policy. For this and other reasons we were prepared to name the Chinese state as the likely responsible party. Chinese officials protested at this; their line was that criminals must have done it. Indeed, the software tools used to penetrate and then remotely control the Tibetans' machines were crimeware tools, freely available on the Internet, and used subsequently by Russian crime gangs. Further details can be found in our technical report, "The Snooping Dragon."¹⁶
30. The Snowden papers inform us that it is also NSA policy that where possible CNE operations should use crimeware tools against targets that might be competent at defending themselves, or be able to call on competent assistance. The main reason is deniability; a secondary reason is that an agency will not want to needlessly risk a

¹² "Measuring the Cost of Cybercrime", Ross Anderson Chris Barton, Rainer Boehme. Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage, *The Economics of Information Security and Privacy*, (Springer 2013) pp 265–300

¹³ "The Cost of Cybercrime", Cabinet Office, 2011

¹⁴ See for example "2007 cyberattacks on Estonia", Wikipedia

¹⁵ "Obama imposes new sanctions against North Korea in response to Sony hack", Dan Roberts, *The Guardian*, 2nd January 2015

¹⁶ "The Snooping Dragon – social-malware surveillance of the Tibetan movement," Computer Laboratory Tech Report TR-746, <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.html>

valuable asset, such as a vulnerability of which no-one else is aware and which can therefore be used to get covert access to high-value adversary systems.

31. The 5 eyes and other governments have been investing in CNE for intelligence, defence and law enforcement purposes at ever-greater scale in recent years. Since the 2010 publicity for the Stuxnet attack on Iran's uranium centrifuge facility at Natanz¹⁷, the market prices for vulnerabilities have surged.
32. This has led to significant unease in the industry about 'vulnerability stockpiling'; that rather than reporting problems with the systems on which we depend, many agencies keep them secret, with a view to using them for offensive purposes.

The vulnerability ecosystem

33. Vulnerabilities can be thought of as the computer equivalent of loopholes in the law. As the law on some subject gets complicated, specialists notice interactions that the lawgiver did not foresee and which may (for example) enable a company to pay less tax. Eventually this is noticed, and once enough firms start using the loophole, the law is changed. In exactly the same way, the software that runs on a computer, phone, car or other device becomes more complex over time as new features are added; eventually, security researchers or others notice that sequences of instructions which the designers had not foreseen have some interesting effect, such as enabling unauthorised programs to be run on the device. If this is exploited at sufficient scale, then eventually the software will have to be changed. This may be expensive: cars may be recalled to a garage for patching, while railway signals may require a visit from a technician.
34. It is expensive to change software, just as it is expensive to change laws. Our society mitigates the cost of law change by leaving many of the rules in regulations that can be changed by statutory instrument, or in CPS or other guidelines that can be changed by order. Similarly, many steps have been taken to reduce the cost of changing software to fix vulnerabilities as they are discovered. Microsoft automatically ships a bundle of patches to Windows PCs every month, and the software of many but not all mobile phones is upgraded regularly.
35. There is also a software industry tradition of responsible disclosure, whereby security researchers or others who discover vulnerabilities report them to the software maintainer in confidence in advance of making them public. For example when our team discovers flaws that could affect banking systems we typically disclose them to regulators (the FCA, the US Federal Reserve, the European Central Bank) who in turn pass the news on to Visa and MasterCard who in turn inform equipment vendors and their member banks. This gives the vendors time to work out how to fix their systems and ship upgrades to their users. Public disclosure might follow 3–6 months after that, or longer depending on

¹⁷ See for example "An unprecedented look at Stuxnet, the world's first digital weapon", Kim Zetter, Wired, 11 March 2014

the circumstances. This convention aligns incentives in that the researcher gets rewarded with publicity while the vendors are pushed to fix the flaw rather than hushing it up. In the case of vulnerabilities in common operating systems and network software, disclosure may be to the vendor, the maintainer, or a computer emergency response team (CERT).

36. This convention is backed up by further mechanisms. First, major systems and software firms such as Google, Apple and Facebook operate “bug bounty” programs, whereby security researchers who report vulnerabilities get paid directly. Second, there have been overt markets in vulnerabilities since about 2003 when iDefense and Tipping Point were set up. Their business model was to report the vulnerability to the vendor but meanwhile warn their own customers, who would enjoy additional protection in the time window between the vulnerability’s being reported and its being finally fixed. This was one of the early industrial applications of the discipline of security economics that I helped found.
37. Since 2000, the 5 eyes powers have enjoyed privileged access to vulnerabilities reported to the CERT system. This was part of a deal that ended the “Crypto Wars”, the struggle between the NSA and the tech industry over the regulation of cryptography, to which I will return later. At the time I was a consultant to Intel and under NDA; the NDA has now expired. The deal as it was reported to me was that the NSA would stop pushing to restrict the use of cryptography in ways that were harming US industry and instead rely on the exploitation of vulnerabilities that occurred naturally. The mechanism is as follows: when a vulnerability is reported to a CERT, it flows through the CERT network to the main CERT in Pittsburgh, which then reports it to the vendor. CERT also has staff with security clearances who also report it to the NSA. So the NSA has advance knowledge of vulnerabilities that have been reported but not yet fixed. (The UK government also set up a UK CERT under the aegis of the Security Service but this is nowhere near as centrally located as the US one, which receives information from CERT teams in thousands of organisations worldwide.)
38. This was how the world worked from about 2000–2010: thousands of vulnerabilities discovered by many people independently would flow to vendors to get fixed; or flow via CERT in which case the NSA, GCHQ and 5 eyes partners got a few months’ exploitable advantage; or flow via vulnerability markets such as iDefense in which case their customers got a few months’ advance protection instead. In either case, within a few months the fix would become available to all.
39. Things changed from about 2010 with the growth of a second generation of vulnerability markets consisting of companies whose customers did not want to get protection, but to do attacks. Companies such as Vupen and Hacking Team started selling to government agencies rather than to corporate America; they either sold hacking tools, that would enable a police force or intelligence agency to take over a suspect’s laptop or mobile phone directly, or they sold vulnerabilities that the agencies could use in their own tools.

40. As a result, the amount of money available to a researcher who found an exploitable vulnerability in Windows or Android or iOS increased from perhaps \$10,000 to over \$100,000.
41. The trade in vulnerabilities can be understood by studying a large cache of emails leaked from Italian cyberweapons manufacturer Hacking Team, in July 2015¹⁸. These emails make their own business practices clear and also contain intelligence on their competitors. According to initial press analyses of the leak, Hacking Team were not just selling malware to NATO governments but to many repressive states, including Russia, the Sudan and Uzbekistan, something they had denied doing¹⁹. The Hacking Team leak followed a hack of a UK competitor, Gamma, in 2014²⁰. These leaks confirmed that the 5 eyes agencies are major purchasers of vulnerabilities and of tools incorporating them.

Effects of CNE preparations on the wider software economy

42. These attempts by NSA, GCHQ and other governments' agencies to acquire and stockpile vulnerabilities have so increased demand as to cause real damage to the software ecosystem. For example, I learned in 2012 that a volunteer to the Webkit free software project, which develops and maintains graphics software for use in browsers, had been discovered trying to sneak a vulnerability into the software, with a view to selling it later. This sort of behaviour was profoundly shocking to the free software community; it might perhaps be compared to a news of a parliamentary draftsman accepting a bribe from a company to insert defective language into a Finance Act so as to create a loophole the company might exploit. While one might expect overt lobbying (e.g. of ministers), a disclosure of covert manipulation of the legislative machinery could significantly undermine trust.
43. Such behaviour had been unknown before it became possible to sell vulnerabilities for six-figure sums, and it poses a real problem for the industry. Much of the software on which we rely is built on free software platforms; FreeBSD is the basis for Apple's operating systems and Linux for Google's, while almost everyone's browser uses Webkit and most of the world's web servers run Apache. Some of this software is provided by companies who want others to use their standards, in order to get commercial advantage elsewhere (for example, Apache was originally written by a consortium of firms including IBM and Hewlett-Packard in order to provide a shared platform to compete with Microsoft). But much is written by volunteers, such as computer science graduate

¹⁸ See for example "Hacking Team: A Zero-day Market Case Study", Vlad Tsirkeivich's blog, 22 July 2015

¹⁹ "Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim", Alex Hern, *The Guardian*, 6 July 2015

²⁰ See for example "Top gov't spyware company hacked; Gamma's FinFisher Leaked", Violet Blue, *ZDnet*, 6 Aug 2014

students, who acquire both skills and reputation capital thereby, rather like law students interning as judges' clerks. It will impose very considerable costs on industry if all contributions to free software projects have to be vetted carefully for malice.

44. For this reason, industry views the stockpiling of vulnerabilities by the NSA, GCHQ and others with great alarm and, in the USA at least, has lobbied hard for a change in policy, particularly after the 2013 Snowden revelations make clear the scale of the program to facilitate CNE. This has now become a sensitive issue in Washington.
45. The industry feeling of violation was exacerbated by the Snowden revelation that GCHQ had been collecting Google traffic in transit between the company's data centres, in order to circumvent the encryption used by default on the links to users. Such network exploitation was seen as a gross breach of trust and left firms determined that law-enforcement access should only be through the front door, by due process of law.
46. The Snowden documents reveal that NSA / GCHQ built significant infrastructure to facilitate global CNE, with references to systems such as FOXACID (for launching malware against targets), TURBINE (to control a network of TURMOIL implants), and WARRIORPRIDE apparently a proxy network of infected machines providing 'scapegoat targets' through which exfiltrated material could be relayed. Technical information is fragmentary but taken together the disclosures suggest that large numbers of innocent people's computers were taken over and used for intelligence or law enforcement purposes without their knowledge or consent.
47. Following the Snowden revelations, President Obama set up a Review Group to advise him what to do about surveillance. The group consisted of three eminent lawyers (Cass Sunstein, Peter Swire and Geoffrey Stone), former counterterrorism tsar Dick Clarke, and former acting CIA Director Michael Morrell. It recommended inter alia that the NSA cease and desist from vulnerability stockpiling; that it should focus on its defensive mission rather than its offensive one, and see to it that vulnerabilities were patched as quickly as possible. President Obama implemented most of the Review Group's recommendations; in this case he did not agree unconditionally but rather ordered the NSA to set up a review process. A former NSA director admitted stockpiling in May 2014²¹ but by November 2014 the administration was claiming that it now kept back only a very small number for offensive use, and reported the vast majority to vendors²².
48. There are further costs that follow from the agencies undermining network and other security standards, for example by restrictions on encryption, and from their preparations and actions to target intermediate systems, from Internet routers to wifi hotspots. These

²¹ "Former NSA chief defends stockpiling software flaws for spying", Andy Greenberg, Wired, 7 May 2014

²² US Gov insists it doesn't stockpile zero-days to hack enemies", Kim Zetter, Wired, 17 November 2014

preparations form part of the same security/intelligence/law enforcement tool chain; compromised routers and weak encryption can be used to insert malicious payloads into the communications between endpoints of interest leading to one of them being compromised, even if the endpoints cannot be compromised directly. I will set out the background to encryption restrictions, and describe their effects; then deal with attacks on network infrastructure.

Restrictions on encryption

49. The Prime Minister recently indicated that he would like to see restrictions on encryption that would ensure it never got in the way of law enforcement and intelligence. President Obama is unconvinced but the Director of the FBI has publicly supported the Prime Ministers position.
50. In response to this, an international group of experts on cryptography, including myself, wrote a paper, "Keys under doormats" which explains in detail why this is a very bad idea. I include the paper as Appendix A. It has been published as an MIT technical report and accepted for the Journal of Cybersecurity.
51. Most of us were members of a previous expert group which in 1997 responded to an attempt by President Clinton to control cryptography with an earlier paper, "The risks and costs of key escrow"²³, which our paper in Appendix A brings up to date.
52. There had been a number of sporadic attempts in the 1970s and 1980s to restrict the civilian use of cryptography by using export controls, by steering research funding away from areas considered sensitive, and by giving key researchers consulting work so as to draw them within the security clearance system. Yet cryptography became steadily more important in key commercial applications including ATM and point-of-sale networks (where I first started working in the field), prepayment utility meters (where I was also a pioneer), software licensing and pay-per-view TV.
53. Cryptography is not just a tool for military and diplomatic communications confidentiality. It provides dependable mechanisms for linking your bank PIN with your account number; for generating the magic code needed to credit your electricity meter; and for ensuring that your software will work, or your set-top box will decipher the football, so long as you pay your subscription. It has become a general-purpose mechanism for taking trust from where it already exists to where it is needed. My expert group colleague and co-author Ron Rivest describes it as being "duct tape". It's what we use to bind digital objects together.
54. The agencies had seen cryptography as their "turf" and now had to watch as it escaped to become a mainstream commercial technology. And control was slowly being lost: the

²³ H Abelson, RJ Anderson, SM Bellovin, J Benaloh, M Blaze, W Diffie, J Gilmore, PG Neumann, RL Rivest, JI Schiller, B Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption", World Wide Web Journal v 2 no 3 (Summer 1997) pp 241-257

agencies had managed to see to it that the Data Encryption Standard, widely used by banks, had a rather short key, and banks realising this started to use multiple encryption. The ever-widening applications of cryptography caused more and more engineers to learn about it and to start contributing innovations.

55. Business for its part became increasingly resentful at the inconvenience and insecurity caused by export controls on cryptographic technology. For example, in 1989 I was working for a large bank in Hong Kong and discovered that the ATM networking there used encryption that was completely insecure. Smart criminals who had wiretapped the ATM network could have deciphered all the passing PINs, recorded the associated account numbers, and forged cards on an industrial scale, possibly forcing the ATM network to be closed. It had been felt impossible to get properly certified hardware encryption devices not just for the network switch but for the 46 member banks; despite the fact that Hong Kong was a British colony at the time, a number of the banks were controlled from mainland China. Eventually the big banks decided to upgrade the cryptography and push hard for the necessary export licenses. At that time, we were suffering substantial credit card fraud by Chinese gangs in the region and needed to introduce CVVs (the 3-digit security codes on card mag strips and signature strips), which are also generated and verified by the hardware encryption devices. Multiple annoyances such as this were creating steady pressure for governments to liberalise cryptography.
56. In 1993, however, the Clinton administration announced the Escrowed Encryption Standard, or Clipper chip. The offer was that firms who switched to this standard would be able to export devices containing cryptography. The catch was that the chip contained an NSA master key, and the design supposedly had the property that encrypted material could be decrypted by the intended recipient, and also if need be by the NSA.
57. In short order, a cryptographer at Bell Labs (Matt Blaze, one of my coauthors on the two crypto policy papers) found a flaw in this design²⁴, and the Clipper chip was abandoned.
58. Several further attempts were made by the US, UK and other governments to come up with technical proposals for controlling commercial cryptography. GCHQ sponsored the development of a key-management protocol for public-sector use, which was shown by a number of academics to have flaws, just like Clipper²⁵. There was a proposal that all cryptographic keys should be put in "escrow" with a "trusted third party"; so all key services would have to be licensed, and a licensing condition would be that the service operator kept copies of the key to hand to GCHQ. The European Commission objected because keys are also used for electronic signature, and third parties with spare copies of

²⁴ "Protocol Failure in the Escrowed Encryption Standard" MA Blaze, Proceedings of the 2nd ACM Conference on Computer and Communications Security: 59–67

²⁵ "The GCHQ Protocol and its Problems" RJ Anderson, MJ Roe, Eurocrypt 97 pp 134–148

keys could forge signatures. Industry objected that government demands to control cryptography were hindering innovation and harming public confidence in e-commerce.

59. While this debate was raging, the UK and US governments prevented the export of cryptography using keys longer than 40 bits. Such keys are weak as they can be found by trying all 2^{40} (about one trillion) possibilities. Longer keys required licenses, so could not be used in mass-market equipment. Licenses were granted only for specific applications such as banking and often only after lengthy and opaque negotiations about the capability of the equipment concerned. This hindered innovation and led directly to serious harm.
60. For example, the content scrambling system used in DVD disks had to use 40-bit keys and as a result was easily broken. This meant that video copyrights could be infringed by illicit copying, and that the region control coding scheme used by the film industry to release new videos at different times in different parts of the world was defeated. This in turn meant that studios had to pay for worldwide marketing of films from the day of release rather than test-marketing them in the USA first.
61. Another example comes from WEP, the first system used to encrypt wifi. Its vulnerability meant that people could get service without paying, and that supposedly secure wifi networks could be penetrated in order to attack devices using them. The most high-profile resulting loss was claimed to have been the theft of over 40 million customers' credit and debit card details from TJ Maxx, millions of which were sold to fraudsters²⁶. The hacker Albert Gonzales was arrested with \$1.65m in cash and got 20 years. The costs to affected companies, including banks who had to reissue compromised cards, were reported in hundreds of millions.
62. Some industries were permitted to use slightly longer but still inadequate keys. For example, the most common contactless smartcard system for many years was the Philips Mifare, variants of which have been used in many systems from the Oyster Card to the door locks on the building where I work. The Mifare card used 48-bit keys and was broken ten years ago. As a result, the Oyster card could be cloned from October 2008 and TfL had to improve back-end systems to detect cloned card use²⁷.
63. Most of the remote key entry systems used in cars have been broken as they use defective cryptography designed in this era; a significant proportion of the theft of high-value motor vehicles in the UK can be traced, directly or indirectly, to the Crypto Wars. Many other vulnerable systems are still in service, forcing system operators to implement system changes or mitigations at great expense, or live with the risk of breakins.

²⁶ "T.J.Maxx Data Theft Likely Due to Wireless 'Wardriving'", Larry Greenmaier, Information Week 9 May 2007

²⁷ "Why being open about security makes us all safer in the long run", B Schneier, The Guardian, 7 August 2008

64. Another victim of weak keys is the authentication in CANBUS, the standard way for components in a car to talk to each other. An attacker who can run malicious code in a car radio (for example) can progressively take over one vehicle component after another, until ultimately they have the engine control unit, the brakes, the accelerator and even the door locks. In 2010, researchers from UCSD and the university of Washington showed they could take over all but the steering wheel of a target vehicle²⁸. This led others to experiment with hacking motor vehicles remotely, and recently to the recall of 1.4 million vehicles by Chrysler after hackers showed they could take over 2014 and 2015 model Jeep Cherokees over the Internet²⁹.
65. Where products supported weak keys for export but strong keys for domestic use in the USA or in 5 eyes countries, the key management mechanisms typically turned out to be vulnerable to attack.
66. One example is SSL/TLS, the protocol used to encrypt traffic to and from websites. Since its introduction two decades ago, this has suffered repeated "downgrade" or "rollback" attacks where an attacker tricks the communicating parties into believing that the other party is using export-grade cryptography. Most recently, the FREAK attack³⁰ targeted export-grade RSA keys, and embarrassingly the vulnerable websites included whitehouse.gov and nsa.gov (in total, over a third of websites were vulnerable including large commercial sites such as American Express and Groupon).
67. Another is the BBK (Barkan-Biham-Keller) attack on GSM, the standard used by mobile phones for authenticating handsets and encrypting both speech and text messages. Again, there was a 'strong' algorithm A5/1 and an 'export' version A5/2³¹. It turned out that an attacker who listens to a conversation encrypted with the former can then replay the authentication protocol later to the handset, asking it to use the latter. The handset generates the same encryption key it used before, and this key can now be solved, enabling the earlier traffic to be read. This vulnerability persists to this day despite the later introduction of an 'even stronger algorithm' A5/3. The result is that foreign intelligence services who maintain sigint facilities in their embassies in London can decipher the mobile phone calls and texts of high-value UK targets.

²⁸ Experimental security analysis of a modern automobile, Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, IEEE Symposium on Security and Privacy 2010

²⁹ "Fiat Chrysler recalls 1.4m vehicles in wake of Jeep hacking revelation", The Guardian, 24 July 2015

³⁰ CVE-2015-0204

³¹ Instant ciphertext-only cryptanalysis of GDM encrypted communications, E Barkan, E Biham, N Keller, Journal of Cryptology v 21 (2008) 392–329

68. Another is the hugely complex design of IPSEC, the protocol used in most virtual private networks (VPNs) on which many companies rely to protect confidential data in transit across public networks. This resulted from the NSA/GCHQ demand to have an export version that does authentication only. Snowden revelations about all VPNs being breakable, and about collection of IPSEC key negotiation traffic worldwide, have since undermined firms' confidence in VPN products.
69. A current topic is BGPSEC. At present, the networks that collaborate to form the Internet trust each others' route announcements, which are not strongly authenticated. Problems can occur when one network announces that it has good routes to certain IP addresses and this causes other networks to send it traffic for those addresses, where this is not appropriate. For example, Pakistan Telecom tried on 24th February 2008 to censor YouTube by announcing that it had good routes to YouTube; this announcement was visible worldwide rather than just in Pakistan, leading to 2 hours and 15 minutes of global service denial. In another incident, China Telecom announced on 8th April 2010 that it had good routes to many US and other addresses, causing about 15% of the world's Internet traffic to flow via China for 18 minutes. Some people thought this was backscatter from a Chinese test of a "cybernuke"; my own view was that it was probably an honest mistake³². Nonetheless it's clear that malicious route announcements could do grave damage to the Internet's routing infrastructure, and in consequence a suite for authentication protocols for interdomain routing, BGPSEC, is currently under standardisation. However BGPSEC doesn't stop route leaks or relay attacks, and some people are concerned that the GCHQ/NSA input to this process is having an effect similar to that on X.509 and IPSEC. To put it bluntly, perhaps the agencies are more concerned with their ability to take out the Internet in hostile countries in times of tension than they are with preventing hostile actors (including terrorists) doing the same to us.
70. The laws and regulations enacted to impose export controls on cryptography also inflict collateral damage. In the 1990s the US pushed the UK to extend export controls from tangible items such as tanks and planes to intangibles such as software. The result was the Export Control Act 2002. This was opposed by research scientists, including then President of the Royal Society Lord May, as it brought under the export control regime not just cryptographic software but software written by academics to control many types of scientific equipment that were subject to export licensing. The effect is that perhaps tens of thousands of academics, as well as tens of thousands of software developers, are technically breaking a law of which most are completely unaware. Those of us who are aware of the law can circumvent it with ease (by putting software in the public domain by making it available on our websites).

³² For a discussion of these incidents and BGP security generally, see "Resilience of the Internet Interconnection Ecosystem", Panagiotis Trimintzios, Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzouios, ENISA, 2011

Indirect costs of GCHQ / NSA controls on commercial information security

71. The persistent attempts by GCHQ and its 5 eyes colleagues to see to it that commercial information security is only just 'good enough' impose serious costs indirectly. For example, during 1995-6 I advised the BMA on the safety and privacy of medical information systems, and one of the issues was whether medical records, test results and so on could be sent by email. After we suggested that personal health information be protected using available free software tools such as PGP, the Department of Health commissioned a report from a consultancy that took advice from GCHQ and recommended a government-use system with key escrow. GCHQ saw this as a means of marketing their key escrow agenda but the technology was inappropriate. First, there is no need for government access to keys when at least one endpoint is always an NHS organisation and the government thus has access to the plaintext anyway. Second, the use of a closed proprietary system cut sharply the number of possible competing suppliers.
72. The end result was first that the NHS initially adopted an obsolete email standard (X.400) which delayed the adoption of proper email in the NHS by several years; second, that BT became a monopoly provider of NHS networking, with the result that the DSL link to a GP practice costs perhaps ten times as much as a similar link supplied by the same company to a vet next door; and third, that for some years the focus of information security in the NHS was keeping out 'hackers' rather than preventing abuse of authorised access by insiders, which is by far the main source of abuse. In short, a misguided GCHQ policy led to NHS networking being late, expensive and insecure.
73. As a second example, I worked on standards for authenticating communications in electricity substations with a student who was sponsored by ABB to work on this problem. The US government had realised that its electricity transmission and distribution infrastructure might become vulnerable to cyber-attack and had pushed the regulators and standards bodies to come up with solutions. Consultants were hired and a proposal, which became draft IEC 62351, according to which communications between devices in a substation would be digitally signed. This was however not implementable as some of the messages between meters, controllers and switchgear must be delivered within 5ms, and the cryptographic processors capable of executing the specified digital signature algorithm quickly enough are subject to US and UK export controls. The standard had to be redesigned to focus on protecting communications from the substation to the network control centre using such mechanisms, while traffic on the substation's local area network would be protected either physically or using message authentication codes that can be computed and verified quickly in software. This whole debacle held up for several years the standards process and thus the prospect of protecting power grids, both in the USA and here, from cyber-attack using standard cryptographic mechanisms.

Deliberately weakening systems to facilitate LE access

74. In addition to the weaknesses in encryption algorithms and protocols described in the section above, there have been sustained and harmful efforts to modify system designs in

other ways to facilitate law enforcement and intelligence access. This is partly done by overt means such as CALEA (the US Communications Assistance to Law Enforcement Act, which enables the US authorities to order the suppliers of communications hardware and software to build in wiretap facilities), and partly by covert deals, of which the most notorious was the backdoored elliptic curve random number generator.

75. In that case, the 'Dual_EC PRNG' was designed by the NSA and standardised by NIST. It was used to generate cryptographic keys. It is now believed that the NSA, knowing secret parameters, can predict the random numbers it generates and thus the keys. As the generator is slower than need be, adoption incentives were needed, and it is reported that the NSA paid RSA Data Security, the main supplier of encryption toolkits to developers, \$10m to embed it by default in its product. The contract between RSADSI and the NSA was among the Snowden leaks. The collateral damage has included the credibility of NIST as a cryptographic standards-setting body; NIST had to abandon proposed changes to the cryptographic hash function SHA-3 as the crypto community is no longer prepared to trust it.
76. It is not only the US government that pushes telecommunications equipment providers to insert wiretap facilities; GCHQ has been doing the same since at least the early 1970s when standards were set for the first electronic telephone exchanges. It cooperates with other agencies in Europe to standardise mechanisms via ETRI. In addition to providing interfaces of signals intelligence agencies to collect traffic, under various warrant regimes, from the operator with its cooperation, such mechanisms are sometimes also exploited covertly, and academic researchers have criticised the quality of security protection engineered around these back doors. In a famous case, law-enforcement access features standardised by ETRI in GSM base station and back-end systems were exploited to hack Greek government mobile phones in 2004 during the Athens Olympics. A team of unknown attackers subverted the wiretap facilities in the network of Vodafone Greece to tap the mobile phones of the Prime Minister, the Minister of Defence and other prominent Greek officials³³.
77. Yet another example of subverting commercial computer-security products was revealed again in the Snowden papers with the story that GCHQ / NSA had been reverse engineering and finding ways to subvert anti-virus software³⁴. The news that security software can also be a vector of infection by state actors can have a chilling effect on normal users' willingness and ability to protect themselves. The cynical may ask whether it's significant that the antivirus firm in the story is a Russian one, which disclosed the existence of Stuxnet. Is this GCHQ / NSA's revenge? Are Western antivirus firms like Symantec and McAfee trusted not to find US / UK government malware? I have no answer to these questions, but once people start thinking in these terms, trust in the whole

³³ The Athens Affair, Vassilis Prevelakis and Diomidis Spinellis, IEEE Spectrum 29 June 2007

³⁴ "GCHQ and NSA broke antivirus software so that they could spy on people, leaks indicate", Andrew Griffin, 23 June 2015

industry is undermined. It becomes more difficult to get people and firms to take even rational action to mitigate real threats from cybercriminals and hostile state actors.

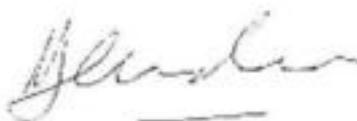
Conclusion

78. In conclusion, GCHQ has been engaged at all material times with the NSA and its other 5 eyes allies in a sustained, directed and generously funded programme to facilitate CNE by restricting the use of strong information security mechanisms such as cryptography, undermining their effectiveness by subverting the design and implementation of cryptographic protocols, random number generators and other essential system components; compelling the introduction of backdoors into infrastructure and other products by manipulating technical standards or as a condition of export licensing; positioning itself in the vulnerability reporting ecosystem so as to take covert advantage of naturally-occurring vulnerabilities reported in good faith for remediation; and subverting the market for vulnerabilities by bidding up the price of exploits that are not thereafter reported to vendors for closure.
79. This had imposed very substantial costs on industry and society as a whole. It has facilitated common criminality such as car theft. It has undermined the confidence of prospective customers overseas in the trustworthiness of security and other products offered by UK suppliers. It has damaged public confidence in the trustworthiness of online services, which imposes direct costs on industry; bank customers are more expensive to service in branches than online, and the same goes for much of the retail sector. In general the indirect costs of security breaches are significantly larger than the direct costs.
80. The equities issue is now discussed openly and frequently in the serious business press, not just the technical community. For example, *The Economist* writes on Sep 13 2015: *"Digital weapons have their drawbacks. Iran's nuclear programme was delayed, not derailed. But they present problems for America's military planners. They involve discovering and exploiting weaknesses which potentially affect everyone, not just America's enemies. The NSA, post-Snowden, is under fire for having deliberately weakened commercial cryptography to ease its espionage efforts. A digital weapon that sabotages power stations could also be discovered and used by America's foes."* As a result, industry has pushed back hard.
81. I would like finally to refer the Tribunal to a report in the *Washington Post*, "Obama faces growing momentum to support widespread encryption", Sep 16 2015, and a leaked National Security Council document discussed therein "Review of Strategic Approaches". The document and the story suggest very strongly that the US Government is moving towards abandoning the policy of pushing for back-door access to systems and instead favouring defence over attack. This is also a position that many eminent former members of the US national security establishment have adopted as the relative costs have become clear. These are not just economic costs but also relate to the West's soft power – our ability to be a beacon for democracy and human rights in a troubled world

must also be balanced against the minor additional gains that might flow to intel and law enforcement if the rules online were to be less onerous than the rules offline.

82. I refer in particular to the statements of former NSA Director Mike McConnell and former Homeland Secretary Michael Chertoff to the effect that despite the legitimate concerns of law enforcement about encryption, "the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."
83. They continue, "The administration and Congress rejected the Clipper Chip based on the reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the '90s and into the new century."
84. The overriding public interest is in protecting the security of the digital infrastructure on which we are all increasingly coming to rely. The actions of GCHQ / NSA have caused, and will continue to cause, damage to that infrastructure and to our computer and communications security more broadly by systematically interfering with security and cryptography – via standards, via export controls, and now via the large-scale deployment of CNE.
85. The US administration thankfully seems to be realising that this was a strategic mistake.
86. I am happy to provide the Tribunal with further information, if so requested, and to appear before it.

Signed



Ross John Anderson

Cambridge, September 30th 2015

IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT 14/85/CH
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT 14/120-126/CH
BETWEEN:

GREENNET LIMITED

RISEUP NETWORKS, INC

MANGO EMAIL SERVICE

KOREAN PROGRESSIVE NETWORK ("JINBONET")

GREENHOST

MEDIA JUMPSTART, INC

CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

EXPERT REPORT OF PROFESSOR PETER MICHAEL SOMMER

1. I am instructed by Bhatt Murphy, solicitors who act for the Claimants, to provide the Tribunal with expert evidence in relation to the technical features of the various forms of Computer Network Exploitation and Equipment Interference. I am asked to provide a description and to indicate the degree of interference with privacy involved in such activities, and issues that may arise in the authorisation and deployment of these techniques and their oversight.
2. For the purpose of this Report my over-riding duty is to the Tribunal and not to those who instruct me. I understand that the Tribunal does not have procedural rules similar to those in the Civil and Criminal Courts but nevertheless I have followed the obligations on Expert Witnesses laid down in Civil Procedure Rule 35 and Criminal Procedure Rule 33 (Rule 19 in the version with effect from 5 October 2015).
3. This Report is aimed principally at addressing elements in Item 6 in the Proposed Legal Issues document of 27 July 2015 and in particular providing factual evidence to support the assumptions that the use of CNE might have involved the following:
 - The obtaining of information from a particular device, server or network. (item a)
 - The creation, modification or deletion of information on a device, server or network. (item b)
 - The carrying out of intrusive surveillance. (item c)
 - The use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest. (item e)
 - The use of CNE to weaken software or hardware at its source, prior to its deployment to users. (item f)
 - The obtaining of information for the purpose of maintaining or further developing the intelligence services' CNE capabilities. (item g)

I understand that item 6(d) is being addressed in a report by my colleague Professor Ross Anderson.

4. In addition the Report also sets out my opinion on the following elements in Item 5:
- What records ought to be kept of CNE activity? Is it necessary that records of CNE activity are kept that record the extent of the specific activity and the specific justification for that activity on grounds of necessity and proportionality, identifying and justifying the intrusive conduct taking place? (item b)
 - What, if any, is the relevance of the fact that, until February 2015, it was neither confirmed nor denied that the Respondents carried out CNE activities at all? (item d)
 - What, if any, is the relevance of the Covert Surveillance and Property Interference Code, issued in 2002 and updated in 2010 and 2014? (item e)
 - What, if any, is the effect of the publication of a Draft Equipment Interference Code of Practice in February 2015? (item f)
 - What, if any, is the relevance of the Intelligence Services Commissioner's oversight of the use of the powers contained within ISA 1994? (item g)
 - What, if any, is the relevance of the oversight by the Tribunal and the Intelligence and Security Committee of Parliament? (item h)

Qualifications

5. I am an academic and cyber security consultant. I have acted as an expert, over the last 20 years, in many criminal and civil proceedings in the UK and elsewhere usually where digital evidence has been an issue including official secrets, terrorism, state corruption, global hacking, murder, corporate fraud, privacy, defamation, breach of contract, copyright breach, professional regulatory proceedings, harassment, allegations against the UK military in Iraq and child sexual abuse. Particular themes have been situations where the Court requires assistance to understand technology and assessments of quantum and extent of damage. I have acted as an expert for the prosecution and defence, for claimants and defendants and have advised governments and individuals.

6. My first degree is in law, from Oxford University. Until 2011 I was a Visiting Professor in the Department of Management at the London School of Economics. I am currently a Visiting Professor at De Montfort University Cyber Security Centre and lecture, examine and validate curricula at other universities. I have been a specialist advisor in the House of Commons and consulted for the OECD, the UN, the European Commission, the UK Cabinet Office Scientific Advisory Panel on Emergency Response, the UK National Audit Office, the Audit Commission and the Home Office. The OECD work, written with Professor Ian Brown of Oxford University, addressed the cyber aspects of Future Global Threats. I have given evidence to the Home Affairs and Science & Technology Select Committees, the Joint Committee on the Communications Data Bill and to the Intelligence and Security Committee.
7. I am the author, pseudonymously, of *The Hacker's Handbook*, *DataTheft* and *The Industrial Espionage Handbook* and under my own name *Digital Evidence*, *Digital Investigations* and *E-Disclosure (IAAC)* now in its 4th edition.
8. During its existence I was the joint lead assessor for the digital speciality at the Home Office-sponsored Council for the Registration of Forensic Practitioners and currently advise the UK Forensic Science Regulator and the Home Office on communications data.
9. I am a Fellow of the British Computer Society and also a Fellow of the Royal Society of Arts.

What techniques are involved in “Computer Network Exploitation” and “Equipment Inference”?

10. Computer Network Exploitation - CNE - means the use of what are commonly called “hacking” techniques in order to gain access to computer-held information. It can also refer to aggressive destructive actions, for example to disable or disrupt a computer resource.

Equipment Interference - EI - refers to a number of related specific techniques; the interference can be to software including operating systems but also to hardware. A related three-letter acronym, CNA, stands for Computer Network Attack, activities designed to destroy or degrade the computer resources of others. The terms are, to an extent, used interchangeably.

11. Equipment Interference, as it appears in the Home Office's Draft Code of Practice ("Draft EI CoP") published in February 2015¹ uses language which, intentionally or not, does not make obvious what in practice is involved. Similarly the Home Office Covert Surveillance and Property Interference Code of Practice of December 2014² appears at first reading to be about authorisations in particular circumstances to enter private premises without saying that frequent reasons for so doing include the planting of devices that will capture activities within those premises via audio and video and transmit the results – by wire, radio, mobile phone or other means – so that they can be heard, and if appropriate, recorded and analysed by investigators. None of the provided examples refer to this.

12. Paragraph 1.6 of the Draft EI CoP refers to the following:

This code applies to (i) any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:

- a) obtain information from the equipment in pursuit of intelligence requirements;
- b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;
- c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);
- d) enable and facilitate surveillance activity by means of the equipment.

¹

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf

²

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interference_web__2_.pdf

“Information” may include communications content, and communications data as defined in section 21 of the 2000 Act

13. The position of the Agencies, referred to in the Proposed Legal Issues document, is that they neither confirm nor deny (“NCND”) their capabilities. One reason for this is that they fear that publication would alert their targets who would then take more effective evasive action³. The problem with this position is that politicians who grant general powers through legislation and Codes of Practice, those who authorise specific activity and those charged with pre- and post-deployment oversight may not have sufficient understanding of the levels of intrusion involved in an application and hence not be able to make informed judgements about necessity, proportionality and issues of collateral intrusion. In addition, as will be seen later, a number of actual acts of exploitation involve several stages of technical activity each of which perhaps ought to be the subject of separate authorisations.
14. It might appear that the only sources of public information about the use of various EI technologies by government agencies are described in the Snowden papers as published by various news outlets and unredacted passages in the Privacy and Security Report of the Intelligence and Security Committee of Parliament (“ISC Report”)⁴ published in March 2015.
15. But there is a substantial literature going back over 40 years on “hacking” and cybercrime techniques. The authors include academics, analysts employed by ‘malware’ (malicious software) detection and security companies⁵, specialists in digital forensics, expert witnesses providing evidence in court and specialist technical journalists⁶. There

³ Respondent’s Open Response paras 4-9

⁴ https://b1cba9b3-a-5e6631fd-sites.googleusercontent.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7crYc43Cbff6kwUhw2tEIXsnPjftY60jAkt2L6dyGPaMXrTny4Sq88aR13DmKI6G7R440yegEMPM0Tgb6vxgrG3gXOtPXChZkVMnXb42oeUg_0HyTWoBIHTC_4TU8nmXF302GtrG5HOZ01qbnAgIR1bzPI2ISows98Q0mRS3OMv4EEENcNmcrQv7ofxOVr9ubqBWfAxvNKydeaucjRnaBLQVz7pIPWmsWDkRAOeRKB8PYqsvJ3-Pf0o5CgG5D4MF1uJm9g&attredirects=0

⁵ For example <https://securelist.com/>, http://www.symantec.com/security_response/

⁶ For example <http://krebsonsecurity.com/>, <https://www.schneier.com/>

are also specialist conference series such as 'BlackHat'⁷ and 'Defcon'⁸ where such techniques are presented and discussed⁸. "Penetration Testers", sometimes known as 'White Hat' Hackers, are technicians employed by businesses to test the security of their systems by employing hacking techniques to an agreed and designed agenda to examine whether the business has proper security procedures and systems. Some collections of tools used by penetration testers are freely available, for example Kali Linux and Metasploit⁹. These are collections of software tools that bring together a range of CNE techniques to allow such techniques to be deployed quickly and easily. These tools are freely available and do not require extensive technical skill to make use of, although a skilled user will obviously be able to do more.

16. Hacking in the non-Agency world may be carried out for a variety of reasons: as a demonstration of technical skill (recreational hacking), as a form of propaganda to draw attention to a political or ideological aim, as an element in perpetrating a crime such as theft, criminal damage and extortion, as a means of industrial espionage, as a means of destroying the reputation of an individual or an organisation, as a means of circumventing copyright protections. People with these different aims may use the same or very similar techniques.
17. GCHQ will be fully aware of this literature both for its own CNE activities and as part of its remit to provide advice on cyber defence via its CESG unit. To put it in a more tabloid fashion – if certain exploit tools can be deployed by 16- and 17-year-olds to significant effect as I have seen in my practice as an expert witness then it would be very surprising if GCHQ were not able to call upon and use similar or better techniques.

⁷ <https://www.blackhat.com>

⁸ <https://www.defcon.org>

⁹ <https://www.kali.org/>. There are also a number of related books, eg *Kali Linux: Assuring Security by Penetration Testing and Mastering Kali Linux for Advanced Penetration Testing*

18. It is thus relatively easy to assist the Tribunal about many of the CNE/EI techniques from open sources. There is no definitive generally agreed taxonomy of hacking methods and, as will be seen, many actual exploits may require more than one hacking technique to achieve success. The paragraphs that follow provide a non-exhaustive overview of some of the most widely-used; there is some unavoidable overlap in some of the descriptions and some exploits can be placed in more than one category. Later I will also refer to some of the “Snowden” slides.

Remote Access: Software

19. The simplest form of unauthorised remote access to a computer is to acquire by some means its sign-on credentials. The means can include “shoulder surfing”, watching a legitimate user, and social engineering tricks¹⁰ such as phishing¹¹, but also information acquired through the examination of paperwork linked to a user. It is also possible to use “brute force” guessing of credentials, the successive trying of possible passwords until one is successful.
20. There are also the results of the deployment on other devices of some of the techniques explained below and where the devices contain the credentials. Armed with the credentials the intruder can then user the computer in exactly the same way as a legitimate user; indeed it may not be possible, from the digital evidence alone, to distinguish between the intruder and the legitimate user.
21. **Personal Computers** Beyond this it is trivially easy to control a personal computer and many other devices remotely across a network including the Internet. Facilities to do so are included in most versions of Microsoft Windows in the form of “Remote Desktop Connection”¹². The main aims are, for example, to allow a user to access an office computer from home or a travelling user to access a

¹⁰ To induce some-one to carry out an action against their interests – see paragraph 68 below.

¹¹ The sending of booby-trapped email and the use of booby-trapped websites.

¹² <http://windows.microsoft.com/en-gb/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7>

home computer, and to allow users to receive remote assistance from a technician. More sophisticated facilities are available via such commercial products as TeamViewer¹³, Logmein¹⁴ and GoToMyPC¹⁵. The essence is that the computer to be remotely accessed needs to have present a small program which can receive and accept remote commands.

22. There are two types of facility – the ability to view and interact with the computer in the same way as a local user, and the ability to see and explore a list of files on the remote computer in much the same way as in “My Computer” or “File Manager”. Files can be downloaded from the remote computer and indeed uploaded to it.
23. The programs mentioned above are overt in their operation and in practice the technical problems for investigators are not the basic facilities but finding ways to make the operation covert. The aspects that need to be addressed are:
 - 23.1. To insert software on to the target computer without being detected; it will need to evade any malware-detection programs likely to be present. The usual mechanisms are via compromised attachments in emails, via code embedded in websites and via compromised USB sticks.
 - 23.2. To hide any sign that the software exists and the device is being remotely controlled – the hiding has to include any on-screen activity but also the presence of untoward files.
 - 23.3. To hide the fact that data is being transmitted from the computer; this will need to evade security facilities such as firewalls.
24. Commercial and hacker programs to achieve these aims are widely available. Hacker programs are also known as Trojans and RATs –

¹³ <https://www.teamviewer.com/>

¹⁴ <https://secure.logmein.com/>

¹⁵ <https://www.gotomypc.com>

Remote Access (or Administration) Tools – and have been in existence for at least 30 years¹⁶. Commercial programs are aimed at businesses concerned about their employees, private investigators and private individuals concerned about partners and family members and at costs from about £60. These programs offer, in addition to the simple remote viewing and file access, the scrutiny of live activity, keystroke monitoring, email tracking, web activity monitoring, and the remote use of microphones and web cameras.¹⁷ This audio and video capability may have the benefit that there is then no need to use conventional bugs of the sort installed under a Property Interference warrant¹⁸. The significance of these will be discussed later.

25. Commercial and hacker programs tend to rely on a mixture of social engineering¹⁹ – tricking individuals into performing actions that assist the intruder, such as ignoring a security alert, or giving up their password and other confidential information – and technical tricks. Often the latter exploit discovered defects in operating systems and application programs. The most sophisticated of these technical tricks are multi-stage – this approach makes detection more difficult. Once a particular defect or bug is known malware detection programs are adapted to find them so that the commercial and hacker programs must constantly be updated in order to remain effective.

26. Thus the secrecy GCHQ may be justified in seeking via NCND is not the basic facts of the possibilities of remote control and remote access but the precise technical methods by which they are achieved.

27. **Forensic Access** A further development of the PC-based activity monitoring programs referred to above is the use of digital forensic

¹⁶ Examples include HakaTak, Blackshades, Back Orifice and many others

¹⁷ Examples include SpyAgent (<http://www.spytech-web.com/spyagent.shtml>), Webwatcher (<http://www.webwatcher.com>), PC Pandora (<http://www.pcpandora.com/>), Spector Pro (<http://www.spectorsoft.com/products/>), and eBlaster (http://www.spectorsoft.com/products/eblaster_windows/).

¹⁸ The audio and video would only be captured in the vicinity of the computer – but the computer may be a laptop or tablet.

¹⁹ See also paragraph 68 below

analysis programs in remote mode. Regular digital forensic analysis programs are able to access the entirety of a hard disk as opposed to those elements that are normally presented to the regular user. Among other things they can perform recovery of deleted data and in some instances restore a disk to a previous state. The major products in this arena can also carry out remote analyses, once an appropriate server has been installed²⁰. In addition they can carry out live interrogations, which may be useful if the target computer is encrypted or is itself accessing other remote services which are password and/or encryption protected. There is also a facility to download a full forensic disk image of a target computer for later, off-line analysis.

28. **Smart phones** The above accounts deal with personal computers. Similar techniques exist for smart phones, though achieving results may require the use of different techniques²¹. Commercial “activity monitoring” software is available²². Smartphone monitoring software can also collect geolocation data, social media activity and SMS text messages.
29. **Tablets** In terms of investigatory issues tablets are very similar to smartphones, lacking only the “phone” aspect; the main operating systems, Android and Apple IOS, are shared between smartphones and tablets
30. **Mainframes** The oldest targets of hacking were large mainframe computers. Most mainframes have remote access facilities and the simplest form of intrusion is to use compromised access control facilities – username and password combinations. Many

²⁰ <https://www.guidancesoftware.com/products/Pages/encase-enterprise/overview.aspx>; <http://accessdata.com/solutions/digital-forensics/ad-enterprise>; <https://www.f-response.com/software/cec>

²¹ <https://www.blackhat.com/docs/us-15/materials/us-15-Trummer-QARK.pdf> and <http://tools.kali.org/hardware-hacking/android-sdk> and <http://www.cnet.com/uk/news/researcher-finds-mother-of-all-android-vulnerabilities/> and <http://9to5mac.com/2015/06/17/major-zero-day-security-flaws-in-ios-os-x-allow-theft-of-both-keychain-and-app-passwords/>; <http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/>

²² For example <http://www.mobile-spy.com/>, <https://mobile-tracker-free.com/>, <http://www.phonesheriff.com/>, <http://www.mspy.com/>

organisations have centralised server facilities – for email, shared files and corporate Internet access. The most popular of the products in use is the Microsoft Exchange Server family – this would be vulnerable to many of the hacks used for Microsoft desktop (Windows) products. The potential “harvest” and also the dangers of collateral intrusion depend on the information held and processed on the mainframe.

31. **Cloud Services** Many individuals and organisations use ‘cloud-based’ services both for data storage and large-scale data-processing. Web-mail, where emails are received and sent via a web-browser as opposed to via a program on a PC and phone and where the archived emails is stored locally, is also a cloud service. Under web-mail emails sent and received are on the cloud’s servers. Access to these services is usually via username/password credentials. Presumably the Agencies will in some circumstances have access via specific or general warrant, but UK law, discussed below, also gives a route via the amendment of s 10 Computer Misuse Act 1990 in s 44 Serious Crime Act 2015 which allows for police and agency use of “computer interference” techniques. The potential “harvest” and also the dangers of collateral intrusion depend on the information held and processed on the cloud service.

32. **“Back-doored” and compromised software** A further route to gaining access to a device beyond those referred to above (see paragraph 23) is to offer enticing programs or apps which themselves contain a hidden Trojan/RAT. They can also contain command-and-control software²³ for BotNets (see below) though a number of those so far uncovered seem directed at fraud and extortion rather than exfiltration of information.

²³ <http://www.computerworld.com/article/2487533/security0/android-trojan-app-targets-facebook-users.html>; <http://www.pcworld.com/article/2360460/trojan-app-encrypts-files-on-android-devices-and-asks-for-ransom.html>; <http://www.v3.co.uk/v3-uk/news/2328691/android-apps-with-trojan-sms-malware-infect-300-000-devices-net-crooks-usd6m>

33. **Mass Remote Control: Botnets** The taking over of a computer and controlling it remotely can be expanded to the point at which very large numbers of poorly protected computers are compromised and herded together in what is called a BotNet (robot network) – a network of compromised computers that can be instructed, *en masse*, to carry out the controller’s instructions. The main criminal use of these botnets is to create a Distributed Denial of Service (DDoS) attack in which a target computer is overwhelmed with large numbers of requests sent by the computers in the BotNet.²⁴ In the cybercrime world these then are often accompanied by demands relating either to some ideological objective or to extortion²⁵.

Website Injection

34. Website injection can consist of planting covert code on a website so that visitors are induced either to give away information about themselves (via a form of social engineering) which can then be later exploited or to receive a Trojan providing backdoor access to their computer²⁶. The website may be genuine and have been hacked or may have been created by the hackers, perhaps to masquerade as a “real” website.
35. Another example is **SQL Injection**. In this the contents of a remote website and more particularly an associated database are downloaded by the use of special commands. Many websites consist of a “front-end” – the pages the users see – and a “back-end”, a database of customer information, orders in progress etc. When a visitor asks the website for information, code on the page translates that into a query

²⁴ There are a number of variants.

²⁵ <http://motherboard.vice.com/read/history-of-the-ddos-attack>;
<http://www.digitalattackmap.com/understanding-ddos/>; <http://www.techrepublic.com/article/chinese-government-linked-to-largest-ddos-attack-in-github-history/>; <http://www.darkreading.com/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787>;
http://www.theregister.co.uk/2014/12/17/london_teen_pleads_guilty_to_spamhaus_ddos/;
https://en.wikipedia.org/wiki/Operation_Payback; <http://www.cnet.com/news/wikileaks-endures-a-lengthy-ddos-attack/>

²⁶ https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

to the database. When the database responds, web page code translates the result into a page which is then seen by the user. Very often the database works to a computer language known as SQL – Structured Query Language. In a poorly protected website, a knowledgeable hacker can craft requests directly to SQL and use that to download all or substantial parts of the database.²⁷

Service Provider Compromise

36. “Service Provider” in this context means a business operating on the web that allows participants to send messages and files, post information about themselves, conduct e-commerce and Internet look-up facilities, picture editing etc.²⁸ The techniques of getting unauthorised access to such services are the same as those mentioned above but because of the volume of personal data likely to be available the consequences are much greater²⁹.

²⁷ <http://www.darkreading.com/risk/sql-injections-top-attack-statistics/d/d-id/11329887>;

<http://www.eweek.com/security-watch/sony-woes-continue-with-sql-injection-attacks.html>

²⁸ Google, Facebook, Amazon, Apple, Twitter and many smaller and less well-known entities all fall into this category so do retail operations with a significant online presence

²⁹ Among significant hacks of this kind: Ashley Madison (<http://www.bbc.co.uk/news/technology-34002915>), Carphone Warehouse (<http://www.independent.co.uk/news/uk/crime/carphone-warehouse-hack-24-million-customers-details-breached-after-cyberattack-10446745.html>), Target (<http://www.businessinsider.com/heres-what-happened-to-your-target-data-that-was-hacked-2014-10?IR=T>)

Hardware Exploits

37. The techniques referred to so far involve software-based exploits. They tend to be easier to deploy as often targets can be induced to install them themselves having been tricked via social engineering. Once the cyber security community is aware of their existence detection software can be written. Hardware-based exploits often require physical access to targets; but their advantages are that software detection tools may not be able to locate their presence and they may also have “persistence”, a feature discussed below.
38. The need for physical access may mean that in some circumstances an Equipment Interference authority will also require one for Property Interference.
39. **Keyloggers** The purpose of a keylogger is to capture and record keystrokes from the legitimate user of a computer. The most common aim is to acquire username/password credentials. Keyloggers are available in software (see paragraph 24 above) but a hardware device consists of a small unit placed between a keyboard and a computer. Commercial versions are available for a few pounds³⁰.
40. **KVMs** KVM stands for Keyboard Video and Mouse and is an item of hardware with a legitimate use of allowing an operator to have one keyboard, video display and mouse which can be quickly switched between several computers. Its main use is by technical staff who may have to manage large numbers of computers. A KVM allows them to use a single keyboard, mouse and display screen, rather than have to have separate devices for each computer. But these devices can be modified to provide hardware-based keylogging and remote access. The technique was used against Barclays and Santander and

³⁰ For example, on Amazon: <http://www.amazon.co.uk/KeyGrabber-USB-KeyLogger-SMB-Black/dp/B004TUBOKW>

referred to in a trial which concluded in 2014.³¹ The modified KVM was linked to a 3G data dongle to allow stolen information to be exfiltrated and bank computers remotely controlled.

41. **PCs** All personal computers have on their motherboard a piece of firmware (software on a chip) the function of which is that when the computer is powered up, the computer is made aware of the hardware – keyboard, display unit, in/out ports, storage devices – attached to it. It then seeks out a storage device, typically a hard disk, CD/DVD drive, USB stick, looking for an operating system. All being well, the operating system is located and the computer is “booted up”. This piece of firmware is known as the BIOS (Basic In Out System). The BIOS is designed to be re-writeable so that, if necessary, the detail of its operations can be subsequently upgraded.
42. It is possible to subvert the process so that the BIOS contains additional features which can include enabling remote access. The advantages of this approach are two-fold. First, regular malware detection only looks at the contents of a hard disk and not any activity before the hard disk is started up. Second, the facility is persistent. The wiping of a hard disk or even its entire replacement will not defeat the BIOS-based program. The use of this technique was much criticised when the manufacturer Lenovo was discovered to have placed persistent advertising software (‘adware’) on some of its laptops³².
43. **Hard Disks** Hard disks consist of the magnetic platters upon which the data is stored, a series of heads which move across the platters to the specific location where the data is stored and some controller hardware which accepts commands from the PC and then directs the heads to read or write the data. The controller hardware can be

³¹ http://www.theregister.co.uk/2014/04/25/kvm_crooks_jailed/;
<http://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hacking-attack-gang-stole-1.3-million-police-say.html>

³² <http://arstechnica.co.uk/information-technology/2015/08/lenovo-used-windows-anti-theft-feature-to-install-persistent-crapware/>

modified so as to create hidden partitions; in fact manufacturers can use this facility to determine the capacity of a disk as sold to the public.³³

44. **USB sticks as vectors of malware** USB sticks are normally used as a low cost small-sized means of storing data and transferring data from one device to another. They can also be used as “boot” devices on PCs – the USB stick contains an entire operating system and the PC is started from the stick rather than the hard drive. One use for this is to “run” an alternative operating system such as Linux while leaving the original hard disk – perhaps with Windows – intact³⁴.
45. USB sticks can be used to insert malware on a PC without the knowledge of the owner by use of the “autorun” facility. When a USB stick is inserted into a PC, the PC will, unless the facility has been deliberately disabled, list out its contents. If among the contents is a file called ‘autorun.inf,’ a program referred to in the file will then immediately run. The facility has a number of legitimate uses but the program may be malware.
46. A more sophisticated version involves reprogramming a USB peripheral so that although it appears to be a storage device it emulates a keyboard and calls a malicious program which could, for example install a back-door. Nothing untoward will appear on screen. This is referred to as “BadUSB”³⁵
47. Many accounts of the Stuxnet malware used to compromise Iranian centrifuges used in nuclear fuel production claim that USB devices were used as the infection vector.³⁶

³³ <https://www.utica.edu/academic/institutes/ecii/publications/articles/EFE36584-D13F-2962-67BEB146864A2671.pdf>; <http://www.stola.com/products/insight/disk-utilities.html>

³⁴ For example: <http://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows>; <http://www.pendrivelinux.com/>

³⁵ <https://srlabs.de/badusb/>

³⁶ <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>; <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

48. **Smartphones** On a smartphone the whole of the operating system is in firmware and can be completely changed. Indeed this is the process when manufacturers upgrade the operating system – many recently-purchased but slightly older Android-based smartphone will have been bought with version 4 of the operating system and then given an over-the-air upgrade to version 5³⁷. On the iPhone and iPad there is a current transition from version 8 to version 9. Although most regular upgrades are over-the-air (via a download from an official site) it is also possible to install an upgrade manually³⁸ and also introduce a new operating system with more facilities than the official one³⁹. In addition mobile phone companies who have sold phones “locked” to their particular network are able to send upgrades and alterations without the customer being aware. This facility gives the opportunity to create a back-door access to smartphones.
49. It is also possible to inject malware, including remote access, via a SIM card. It appears that the injection has to be made or be carried out with the co-operation of the mobile phone company⁴⁰.
50. **Wifi Access Points** Most customers of Internet broadband facilities receive their services through a device called a hub which combines a modem to connect via a telecommunications service (telephone, cable) and a means of internal distribution via a local area network. Often the internal distribution is via wifi. Many retail outlets, coffee shops, hotels and travel locations – airports, train stations – offer Internet access via wifi hotspots⁴¹. The devices which perform this function are all designed to be upgradeable⁴²; just as with PCs and

³⁷ In fact there are usually a number of minor upgrades to each major version.

³⁸ <http://xda-university.com/as-a-user/android-flashing-guide>

³⁹ For example Cyanogen: <http://www.cyanogenmod.org/>

⁴⁰ <http://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/>; <http://www.theverge.com/2015/2/24/8101585/the-nsas-sim-heist-could-have-given-it-the-power-to-plant-spyware-on>

⁴¹ In 2013 one major UK supplier, The Cloud owned by BskyB claimed that 10 m UK adults logged on to one of its sites every week. <http://www.ispreview.co.uk/index.php/2013/04/10-million-britons-a-week-logging-on-to-public-wifi.html>

⁴² <http://www.thegeekstuff.com/2009/06/how-to-upgrade-linksys-wireless-router-firmware/>

smartphones, the upgrade facility can be subverted⁴³. A common criminal application is the so-called “evil twin”, a subverted device which appears legitimate, entices users to log on but is able to intercept traffic passing through it.⁴⁴ This route would also be useful to Agencies and law enforcement in circumstances where an interception warrant on a communications service provider under RIPA Part 1 Chapter 1 was for one reason or another difficult to obtain, for example where premises were thought to be used to share and download information but there was incomplete information about all possible users such that they could be identified.

51. **Switches** Physically the Internet consists of a series of cables and switches; the function of the switches is to direct Internet packets – information traveling over the Internet - towards their destination. The switches also collect information about network conditions so that packets can if necessary be rerouted via less congested paths⁴⁵. The cables and switches vary considerably in their capacity –smaller for local traffic, very large for traffic between continents. Most switches are remotely accessible and upgradeable for routine management purposes but this provides a means of subverting the facilities so that interception of traffic can take place. In addition, by prior arrangement with the manufacturers it would be technically easy for special Agency facilities to be added. Alternatively products could be intercepted between supplier and customer and the switch firmware modified. One of the leading manufacturers has recently warned of rogue firmware⁴⁶.

⁴³ <http://www.dd-wrt.com/site/index>

⁴⁴ <http://netsecurity.about.com/od/secureyourwifinetwork/a/The-Dangers-Of-Evil-Twin-Wi-Fi-Hotspots.htm>; <http://www.techrepublic.com/article/minimizing-the-threats-of-public-wi-fi-and-avoiding-evil-twins/>; <https://www.youtube.com/watch?v=LwEjYL6Eoro>

⁴⁵ Specification of products by a leading manufacturer can be seen at: <http://www.cisco.com/c/en/us/support/index.html?overlay=switches>

⁴⁶ <http://tools.cisco.com/security/center/viewAlert.x?alertId=40411>

Man in the Middle (MITM) Exploits

52. **Encryption Defeat** The basic aim of a common form of man-in-the-middle (MITM) exploit is to overcome situations where data in transmission is encrypted. The technique consists of interposing a device between the two communicating parties; each believes themselves to be communicating with the other but their traffic is being intercepted before being passed on. In the most common forms of encrypted traffic transmission, the devices being used by the two parties exchange authentication information between themselves, usually via a digital certificate. Once the authentication has taken place a session key is created to carry out the encryption of the subsequent traffic. Different session keys are created for each "conversation" and it is this feature that makes regular interception difficult.
53. The MITM device has knowledge of the respective digital certificates and is hence able to provide apparently satisfactory authentication to both parties. Digital certificates can be obtained by several means – previous "hack" of users' computers where the certificates will be stored, or by compromising the authorities that issue the certificates⁴⁷⁴⁸. Other forms of encryption defeat are discussed below at paragraph 58 below.
54. **Rogue Wifi Access Points**, referred to above at paragraph 50 can also be categorised as a form of MITM attack.
55. **IMSI Catchers** An IMSI catcher is a device designed to identify and capture mobile phone traffic. It is also known as a Stingray, which is the name of one of the available products. It consists of a fake mobile telephone base station and mobile phones in its vicinity are induced by virtue of the strength of the signal it puts out to log on

⁴⁷ <http://arstechnica.com/security/2015/08/attackers-are-hijacking-critical-networking-gear-from-cisco-company-warns/>

⁴⁸ See for example, the compromise the Dutch certificate authority DigiNotar. <https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170>

to the fake station as opposed to an official one provided by a regular mobile phone company. The fake base station intercepts traffic before passing it on to a legitimate base station which is part of the general telecommunications network⁴⁹. There have been accusations in the United States that IMSI catchers have been used by law enforcement as a means of by-passing the warranting procedures for interception⁵⁰. A possible use in the UK by the Agencies and law enforcement is to identify hitherto unknown mobile phones operating within a small physical area of interest.⁵¹

Encryption Defeat

56. A frequent requirement of hackers and cybercriminals is the ability to defeat encryption. Encryption can be software based, as when files are protected but is also deployed in hardware, often to provide copyright protection but also to control access to hardware such as computers, smart phones and data storage devices such as hard disks and USB sticks.
57. Robust encryption of any kind is difficult to defeat but many forms of encryption are not robust – either the encryption algorithm has weaknesses or the overall cryptosystem has been poorly managed so that encrypting passphrases or cleartext versions of files can be located.
58. Encrypted data in transmission can sometimes be defeated via a Man In The Middle attack. See paragraph 52 above.

⁴⁹ <http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>; <https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf>; <https://www.youtube.com/watch?v=3oHx0zj3GWQ>;

<https://www.youtube.com/watch?v=rXVHPNhsOzo&index=5&list=PLD479F2812AE804DD>
⁵⁰ <http://arstechnica.com/tech-policy/2015/04/county-prosecutor-says-it-has-no-idea-when-stingrays-were-used-so-man-sues/>

⁵¹ This would be an alternative to the a “tower dump” from a mobile phone provider as the official tower may not be in an optimal position and may identify many irrelevant and innocent mobile phone subscribers.

59. For file decryption there are a number of commercial products, for example Passware⁵² and Elcomsoft⁵³. These “know” about weakness in popular encryption systems and/or use “brute force” and “rainbow tables” (a method where much of the computational work needed to break a password is done in advance and stored in a large database, making the cracking process much faster)⁵⁴. Software is also available to remove the copy protection from entertainment DVDs and BluRay disks⁵⁵.
60. There have been cases where copy-protected software has had the protection removed so that it can be freely distributed and used via hacker websites⁵⁶.
61. Hardware exploits have, in the cybercrime world, been concentrated around compromising games machines so that they can play more than officially supplied (and encrypted) games and compromising equipment for the reception of satellite and cable tv services so that encrypted programmes can be viewed without payment to the official suppliers⁵⁷.
62. A further area of activity has been to compromise the ink cartridges used in some printers and where the official supplier has designed the printer so that it will only work with cartridges from the original manufacturer.
63. There has been a debate suggesting that GCHQ and NSA have sought artificially to weaken encryption facilities in order to gain easier access to data. I believe that this is the subject of a separate Expert Report before the Tribunal from Professor Ross Anderson.

⁵² <http://www.lostpassword.com/>;

⁵³ <http://www.elcomsoft.co.uk/eprb.html>

⁵⁴ Eg <https://www.freerainbowtables.com/>; <http://kestas.kuliukas.com/RainbowTables/>

⁵⁵ <http://www.winxdvd.com/resource/best-free-dvd-decrypter-software-review.htm>

⁵⁶ Eg DrinkorDie, http://www.theregister.co.uk/2005/05/06/drinkordie_sentencing/

⁵⁷ <http://forums.xbox-scene.com/index.php?topic/653015-mrmodchips-wins-appeal-in-1m-gbp-uk-modchip-case/page-3>

Reverse Engineering

64. Reverse engineering involves the processes of examining a product, hardware or software to see how it operates, often for the purpose of creating an alternative means of producing the same result. In the “open” world there are two main reasons for utilising the techniques; the first is to circumvent intellectual property rights. The second, often used by malware analysts, is to seek to understand the inner workings of an item of malware, partly as a contribution to general knowledge but also to develop detection and mitigation products.
65. In the hacker world, as already mentioned, reverse engineering is used to thwart copyright protections on hardware such as games consoles and satellite and cable set-top boxes.
66. Reverse engineering can also be used in seeking to thwart security products, including those for access control. One area where there has been significant “cybercrime” activity is the reverse engineering and compromise of credit and debit card Point-of-Sale terminals as used in retail outlets⁵⁸.
67. I will refer later to reverse engineering as part of the skillsets and research endeavours of GCHQ and its partner NSA.

Social Engineering

68. At several points in these descriptions of hacks reference has been made to social engineering. In order to give the activity sufficient prominence I am repeating its importance in many hacking / cybercrime events. There are also implications for how its deployment is dealt with in Codes of Practice and in the authorisation and oversight regimes, a matter I return to later in paragraphs 101 and 112.

⁵⁸ <http://arstechnica.com/security/2013/12/credit-card-fraud-comes-of-age-with-first-known-point-of-sale-botnet/>; <http://krebsonsecurity.com/2011/05/point-of-sale-skimmers-robbed-at-the-register/>

69. As already mentioned, social engineering can encompass a deceptive email and website but it may be no more than a “pretext call”, a phone call to an unsuspecting individual. Some security professionals use the phrase “Advanced Persistent Threat” or another phrase “spear phishing” to identify attempts which have been specifically aimed at individuals who are thought likely to have significant administrative roles and who, if their identities are compromised, will yield important technical facilities for later exploitation. The targeting usually involves researching the life of the individual through open sources and social media so that when a booby-trapped email is sent to them it is crafted so they are less likely to be suspicious (for example, a person known to be a theatre lover may be more likely to open a compromised email purporting to contain a discount offer from the National Theatre).
70. The centrality of social engineering in hacking can be seen from books written by a famous serial hacker, Kevin Mitnick, *The Art of Deception, The Art of Intrusion, Ghost in the Wires*⁵⁹. Other books include *Unmasking the Social Engineer* by Christopher Hadnagy⁶⁰ and *Kingpin* by Kevin Poulsen⁶¹. There has also been extensive discussion of social engineering techniques at specialist conferences.⁶²

Multi-Stage Exploits

71. Many of the actual exploits and crimes referred to above have, to be successful, required the deployment of a series of techniques in succession. Examples include:
- Bank credentials obtained by looking over a shoulder or back-door entry to a computer, then used to masquerade as a legitimate in order to siphon off funds. In practice one person may steal bank credentials, offer them for sale via a hidden “Darknet” market place; the buyer may then hire a series of mules to rob the

⁵⁹ http://www.amazon.co.uk/s/ref=nb_sb_ss_c_0_13?url=search-alias%3Dstripbooks&field-keywords=kevin+mitnick&prefix=kevin+mitnick%2Caps%2C145

⁶⁰ Wiley, 2010 and 2014

⁶¹ Random House 2012.

⁶² http://www.cl.cam.ac.uk/events/decepticon2015/conf_program.html

individual accounts and/or launder them via casinos and retail purchases⁶³

- Email credentials acquired by back-door entry to a computer; later used to generate a plausible email to deceive third parties to perpetrate a fraud or as a stage in obtaining confidential information, or as a means of gaining high level access to computer resources
- Small malware program calls another which calls another – an effective technique for making detection difficult
- Malware introduced together with data destruction program either to cause direct damage or for extortion
- Large numbers of computers back-doored and taken over, subject to the command-and-control of a botnet, used for a DDoS attack, followed by an extortion demand.

CNE and EI as a means of attack

72. Strictly speaking the use of CNE /EI for attack purposes is not an “investigatory power” but it may be useful to indicate the main forms that it can take:

- **Remote data wiping** in which stored data is by command over-written beyond recovery
- **Distributed Denial of Service attacks** in which large numbers of innocent third party computers are taken over and placed under command and control. From these, large-scale simultaneous requests can be sent a target computer so that it is overwhelmed and cannot function
- **Targeted attacks** where specific devices are identified, their characteristics examined and attacks crafted so as to disrupt or destroy their capabilities. The best known example of this is

⁶³ NHTCU/SOCA Operation Euphroe, 2005-2007, *Dark Market*, Mischa Glenny, Vintage 2011; Kingpin, Kevin Poulson, Crown, 2011

Stuxnet which was aimed at machinery controlling centrifuges allegedly used by the Iranian authorities to refine uranium

- **“False flag” activities** where a computer resource is created either for propaganda or attack purposes but is controlled by some-one other than the apparent owner. In the alternative, a genuine computer resource is taken over, hijacked, and rogue information and activity is promulgated from it.

Techniques revealed in Snowden documents

73. I now turn to indications in the Snowden papers of the use by GCHQ of a number of specific techniques. The Tribunal will be familiar with how Snowden distributed the material he had acquired and exfiltrated. He did not publish directly but gave copies to a number of journalist outlets including *The Guardian*, *New York Times*, *Washington Post*, *Der Spiegel* and *The Intercept* leaving to them to decide what to publish and when. I am not aware of any suggestion that the files and documents he supplied were forged or inauthentic but I am aware that GCHQ have said informally that some interpretations placed by the media on the materials are incorrect or incomplete and that some of the slides were for informal internal discussion and do not necessarily reflect firm GCHQ policy. In using this material I have sought to be relatively conservative – the references are to slides which have been published and what appear to be reasonably authoritative journalistic articles that have accompanied them, and where the technology used reflects my understanding of what is already known to be possible in the non-Agency world.

74. For the avoidance of doubt, I have not had access to any slides that have not been published and it is quite likely that there are slides which have been published which I have not seen because I am currently unaware of their existence. It has not always been possible to

identify which activities are specific to GCHQ as opposed to NSA; however the 5-Eyes Agreement suggests very close levels of technique and information sharing.

75. The material reviewed here was selected on the basis that they were likely to assist the Tribunal in its deliberations on legality and adequacy of codes of practice and oversight and in particular in framing questions to GCHQ in closed proceedings. Up to a point it makes little difference whether a technique is being deployed as opposed to being the subject of research as what is relevant is what law, codes and oversight permit.
76. The slides often refer to thematic programmes of research and activity and may cover more than one technique. In addition, as already observed many hacking/CNE/EI actions require the deployment of more than one technique, what has been referred to above as “multi-stage exploits”.
77. **NSA Tailored Access Program** In December 2013 *Der Spiegel* published a series of articles about a catalogue of technologies and devices⁶⁴. I produce copies as PMS/1-4. There is a useful Wikipedia listing of some of the techniques⁶⁵ and I produce a copy of this as PMS/5. I produce extended extracts from the ANT Catalog as PMS/6. Among those referred to and by way of example are (the footnotes point to the “open” versions referred to earlier in this Report):
- 77.1. Candygram, which appears to be a IMSI Catcher⁶⁶
 - 77.2. Cottonmouth, which used USB connections⁶⁷
 - 77.3. DeityBounce, which is hardware-based persistent Trojan directed at Dell servers⁶⁸

⁶⁴ <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>

⁶⁵ https://en.wikipedia.org/wiki/NSA_ANT_catalog

⁶⁶ See paragraph 55 above

⁶⁷ See paragraph 44 above

- 77.4. Dropoutjeep, which is software giving remote access and control of Apple iPhones⁶⁹
- 77.5. Feedthrough, a backdoor to some mainframe computers⁷⁰
- 77.6. Ginsu, hardware based persistent remote controller for personal computers⁷¹
- 77.7. Gopherset, software deployed via a mobile phone SIM⁷²
- 77.8. Howlermonkey, remote control of computers via radio⁷³
- 77.9. Iratemonk, compromise of hard disks from certain manufacturers⁷⁴
- 77.10. Ironchef, compromise of the BIOS on a personal computer⁷⁵
- 77.11. Picasso, software that covertly sends data from a targeted mobile phone about location, call data and can also activate the phone's microphone to capture local conversations⁷⁶

78. GCHQ's Technical Enabling Covert Access Product Centre (TECA) In June 2015 The Intercept published what it claimed were details of GCHQ programs to subvert widely-used commercial software⁷⁷. It also included part of a memo describing the services of GCHQ's TECA which I produce as exhibit PMS/7. Also published were a memo on Software Reverse Engineering⁷⁸ which I exhibit as PMS/8 and another memo on Reverse Engineering⁷⁹ more generally which I exhibit as PMS/9.

⁶⁸ See paragraph 41 above

⁶⁹ See paragraph 28 above

⁷⁰ See paragraph 30 above

⁷¹ On the same principles as paragraph 40 above

⁷² See paragraph 49 above

⁷³ Another version of what is described in paragraph 40 above

⁷⁴ See paragraph 43 above

⁷⁵ See paragraph 41 above

⁷⁶ See paragraph 28 above

⁷⁷ <https://firstlook.org/theintercept/2015/06/22/gchq-reverse-engineering-warrants/>

⁷⁸ <https://firstlook.org/theintercept/document/2015/06/22/software-reverse-engineering-gchq>

⁷⁹ <https://firstlook.org/theintercept/document/2015/06/22/reverse-engineering-gchq-wiki/>

79. **JTRIG / SIGDEV** In February 2014 the Intercept published an article on GCHQ's social engineering research⁸⁰. It includes a GCHQ presentation entitled "The Art of Deception"⁸¹. I exhibit this as PMS/10.

80. **I Hunt Sys Admins** In March 2014 the Intercept published a document advising on the value of targeting system administrators as a way of getting access to important computer resources⁸². I exhibit this as PMS/11.

81. **Man in the Middle attacks** A further document from the Intercept published in March 2014 describes techniques very similar to those covered above in

82. **Word did not find any entries for your table of contents.**

In your document, select the words to include in the table of contents, and then on the Home tab, under Styles, click a heading style. Repeat for each heading that you want to include, and then insert the table of contents in your document. To manually create a table of contents, on the Document Elements tab, under Table of Contents, point to a style and then click the down arrow button. Click one of the styles under Manual Table of Contents, and then type the entries manually.s 19, 34 and 52. They are called Willowvixen and Seconddate. I exhibit this as PMS/12.

83. **Quantum Theory** This series of slides⁸³, also from the Intercept in March 2014 shows that NSA/GCHQ tactics often involve multiple stages and can be compared with the "open" techniques covered in paragraph 71 and below. It will be seen that there are explicit

⁸⁰ <https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/>. See also: <http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361>; <http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-british-spies-used-sex-dirty-tricks-n23091>

⁸¹ <https://firstlook.org/theintercept/document/2014/02/24/art-deception-training-new-generation-online-covert-operations/>

⁸² <https://firstlook.org/theintercept/document/2014/03/20/hunt-sys-admins/>

⁸³ <https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/>

references to GCHQ and to the NSA/GCHQ station at Menwith Hill, North Yorkshire. I exhibit this as PMS/13.

84. Purchase of specialist software to facilitate eavesdropping on PCs and mobile phones In June 2014 Wired magazine published a long article about a company called Hacking Team and its Remote Control System⁸⁴ and claimed that this was an instance of GCHQ's purchase of surveillance software. The essential methods are similar to those described above in paragraphs 23, 25 and 28. I exhibit this as PMS/14.

85. Optic Nerve, Webcam Image Gathering, Facial Recognition In February 2014 The Guardian ran a feature on Optic Nerve, said to be a GCHQ program to collect and then process millions of images from Yahoo's use of webcams⁸⁵. I exhibit this as PMS/15 – it includes screen captures said to come from the Snowden archive. In May 2014 the New York Times wrote about the capture of webcam images more generally and their processing using facial recognition software⁸⁶. I produce this as PMS/16. This is a very large-scale implementation of what is available in the open retail market and mentioned above at paragraph 24 above.

86. Auroragold: Cellphone Surveillance In December 2014 the Intercept published an article and slides about NSA's alleged spying on large numbers of cellphone companies world-wide in order to understand their systems and to capture the traffic of their customers⁸⁷. As well as describing something which seems analogous to the PRISM program which targeted Internet traffic the program is also an illustration of multi-stage attack in order to achieve a desired end. I produce the article as PMS/17, the slides for the project overview as PMS/18, slides with more details as PMS/19,

⁸⁴ <http://www.wired.com/2014/06/remote-control-system-phone-surveillance/>

⁸⁵ <http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo>

⁸⁶ http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=0

⁸⁷ <https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/>

slides providing a “working aid” as PMS/20 and a slide which appears to show GCHQ involvement as PMS/21.

87. Gemalto: Breaking Encryption on mobile phone SIM cards.

Another route to getting access to encrypted mobile phone conversations on a mass scale was described by the Intercept in February 2015⁸⁸. This is another multi-stage attack – the first target was Gemalto, manufacturers of SIM cards; information obtained was then used to compromise individual SIMs and the phones in which they were located. I produce the article as PMS/22 and two GCHQ slides as PMS/23 and PMS/24.

88. Belgacom In September 2013, Der Spiegel, relying on Snowden documents, claimed that Belgacom, the Belgian telecommunications company had been the subject of a complex attack by GCHQ under the name “Operation Socialist”⁸⁹. One of the techniques used was “Quantum Insert”, presumably a variant on “Quantum Theory” referred to above at paragraph 83. The technique itself is multi-stage but the apparent reason for targeting Belgacom was that through it there was access to its partners including those in Switzerland and South Africa and through these in turn to actual persons of intelligence interest. In December 2014 the Intercept ran a more extended article claimed to be the “full story”⁹⁰. The Intercept account claims the use of another GCHQ-developed multi-stage approach called Nocturnal Surge. I produce the Spiegel article as PMS/25 and the Intercept article as PMS/26.

89. Karma Police In September 2015, the Intercept published a long article about a GCHQ programme said to have the ambition of capturing the Internet browsing habits of every visible user on the Internet⁹¹. Accompanying the article is a collection of slides and

⁸⁸ <https://firstlook.org/theintercept/2015/02/19/great-sim-heist/>

⁸⁹ <http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html>

⁹⁰ <https://theintercept.com/2014/12/13/belgacom-hack-gcbq-inside-story/>

⁹¹ <https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/>

- 92.1. Directed Interceptions: where the CNE/EI collects traffic – data, audio, video – by compromising equipment rather than via a Communications Service Provider (CSP). These overlap with the functionalities of bugs and taps which are traditionally dealt with via Property Interference warrants in that cameras and microphones can be activated. Such interceptions are targeted at identifiable individuals.
- 92.2. Directed Computer intrusions – with the aim of viewing the contents of a computer, smart phone, etc. Targeted at identifiable individuals.
- 92.3. Computer intrusions to acquire information for later exploitation. Examples include the “I hunt sys admins” document⁹³ and the attacks on the SIM manufacturer Gemalto to break encryption generally⁹⁴ and on Belgacom to gain widespread access facilities⁹⁵.
- 92.4. Mass computer intrusions to collect large quantities of data which might later yield intelligence but without any specific target in mind. Examples include Optic Nerve⁹⁶, a program to collect large numbers of webcam images for later use with facial recognition software and Aurorogold⁹⁷, surveillance of cellphone companies to ease later interceptions of phones.
- 92.5. Computer intrusions with the aim of using facilities to reach other computers and to masquerade as someone else.
93. Looking at these in more detail from the perspectives of levels of intrusion and judgements involved in initial authorisation, on-going management and post-event review/oversight:

⁹³ See paragraph 80 above

⁹⁴ See paragraph 87 above

⁹⁵ See paragraph 88 above.

⁹⁶ See paragraph 86 above

⁹⁷ See paragraph 86above

94. **Non-CSP interceptions** In an interception carried out by a Communications Service Provider in the UK it is likely to use equipment designed specifically for that purpose. RIPA s 12 requires the “maintenance of an interception capability”. This will limit what is acquired by reference to a phone number, ISP subscriber or similar. But where interception is carried out by other means rather more may be collected as there is no obvious technical means of limitation. This is an issue in item 6(e) of the Proposed Legal Issues. Some of the activities considered below come very close to the issues of bulk intercepts. With that one finds oneself re-visiting the view that “interception” does not take place at the point of capture but only when material is read, as reviewed in IPT/13/77/H. I understand that the IPT’s decision is likely to be reviewed before the CJEU.

94.1. A **Wifi Access Point** or **Hot Spot**⁹⁸ will capture all traffic that signs on to it. It will not be possible to filter on the basis of IP address – because a person of interest may be using a dynamically assigned IP address⁹⁹. The investigator requesting the use of a compromised Wifi access point will thus have to carry out post-capture removal of all “irrelevant” material; it is not clear how this process can be controlled and monitored.

94.2. Similar considerations apply to a compromised **Network Switch**¹⁰⁰. It too will capture all traffic that signs on to it. It will not be possible to filter on the basis of IP address – because a person of interest may be using a dynamically assigned IP address¹⁰¹. Again, post-capture filtering of traffic will be required.

⁹⁸ See paragraph 50 above

⁹⁹ Most ordinary users of the Internet do not have a permanent IP address; because of the shortage of such addresses, ISPs usually lease an IP address to a customer for a short period and may share a single IP address between a large number of users.

¹⁰⁰ See paragraph 51 above

¹⁰¹ Most ordinary users of the Internet do not have a permanent IP address; because of the shortage of such addresses, ISPs usually lease an IP address to a customer for a short period and may share a single IP address between a large number of users.

94.3. As we have seen, the main purpose of an **IMSI Catcher**¹⁰² is to identify unknown phones in a particular locality. The process collects all the phone numbers – and possibly also the content of conversations - in the vicinity and again post-capture filtering is required.

94.4. In relation to Optic Nerve and Aurogold, the available slides do not tell us about how the harvest is managed once acquired – the slides are about technical capabilities

95. **Multi-stage Investigations:** A common characteristic of digital investigations is that several stages of technical inquiry may be needed. For example a keylogger may be used to acquire a username/password combination which is then subsequently used to access a computer or a cloud resource. One would want to ensure that any authorisation procedure saw this as two distinct actions. Some of the issues commented on by the Tribunal in the Chatwani/NCA case¹⁰³ where a search warrant was used as a cover for the planting of a bug, may be apposite.

96. **Computer and Cloud Storage Intrusions** Whereas it is relatively easy to forecast the scope of the likely “harvest” associated with an interception the same cannot be true of entry into a computer. I have been examining for forensic purposes personal computers for over 20 years. Most of these have been the result of seizure by the police under PACE and similar powers or where the owners have given permission. The following issues of limiting the level of intrusion arise:

96.1. Most forms of computer access are “all or nothing” either to a computer/smartphone itself or to the user space of an individual account holder.

¹⁰² See paragraph 55 above.

¹⁰³ Case No: IPT/15/84/88/CH

96.2. In the case of forensic access as referred to in paragraph 27 above, the access is so complete as to include portions of the computer that would not normally be seen by the regular user. ACPO Good Practice, which may or may not be applicable to Agency operations, recommends forensic disk imaging¹⁰⁴. Redaction of a forensic disk image is difficult to achieve without losing evidential integrity. In the Criminal Justice world this can create difficulties where, for example, there is material likely to be subject to legal professional privilege.¹⁰⁵ The usual practice is to appoint an independent lawyer, perhaps accompanied by a technician, to arbitrate on what can and cannot be used. But this may be more difficult in an Agency environment where finding the lawyer and technician with the appropriate security clearances and the necessary independence may be challenging.¹⁰⁶

96.3. A "personal" computer these days is just that: a repository of vast amounts of personal information generated by the user. This is even more true of a smartphone which is likely to be with its owner all the time that the owner is awake. This fact of course makes the personal computer such a valuable potential source of evidence but also creates substantial difficulties when applying the necessity, proportionality and collateral intrusion tests.

96.4. Among the classes of information likely to be found are:

- Archives of emails sent and received during the "lifetime" of the device (that is, since it was first used) and possibly copies of emails from previous earlier devices. The position is thus very different from the interception situation where the "harvest" is limited to the duration of the warrant. Emails are not stored individually by the major email programs but in databases¹⁰⁷ which have initially to be acquired in their

¹⁰⁴ <http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf>, paragraph 2.2.4

¹⁰⁵ Attorney General's Guidelines on Disclosure, December 2013, A28-34

¹⁰⁶ The draft EI CoP attempts to address these issues in Chapter 3.

¹⁰⁷ Microsoft Outlook emails are stored in PST files, Thunderbird emails are in "Profiles"

entirety. The emails are highly likely to involve much more than the subjects of immediate interest to an investigator and will of course contain correspondence with individuals against whom there is not and never will be suspicion.

- A routine task of a digital forensic investigator is the examination of the Internet cache (history). Again the cache has to be available to be reviewed in its entirety. Searches may reveal many irrelevant matters that a user wishes to keep private. In one case in which I was instructed an individual was charged and later found not guilty of conspiring to rob a gold bullion truck, and where there were clear indications of his use of sex escort sites in his Internet cache.
- Similar considerations apply to records generated by the use of social media sites, messaging systems and Internet telephony. Records may exist for the entire lifetime of the device.
- Computers also typically contain large repositories of files of various kinds. These can include documents generated by the owner and others, still and video photos, spreadsheets and others. Video material is highly likely to be found on smartphones and tablets because these devices have in-built cameras. Again although some of this material may be of significant intelligence value other files may be irrelevant but intensely personal. In my experience over 60% of computers owned by men are likely to contain sexual material (and I exclude those where the subject of a charge is a sexual offence); pictures may include the computer owner engaging in sex with a partner.
- Personal computers and smartphones often contain credentials for banking and e-commerce and other services. Some of the credentials could be used by investigators to masquerade as the person who owns the computer. As above, one would

want to see that procedures clearly balance the possible intelligence value of this information against normal expectations of privacy.

- Computers owned by families may have several user accounts for different family members; all user accounts not just that of a suspect would be open to scrutiny by investigators.
- In the case of computers used to run a business it is very likely that there will be a database of customers, this in turn may include credit and other financial information. In any event the database will probably fall within the remit of Data Protection legislation and contain information personal to the individuals within it.

97. Active Use of Computers This is the situation where a third-party's computer is taken over and used to carry out further actions:

- 97.1. At a technically trivial but important level, these techniques can be used to disguise GCHQ's involvement in intelligence gathering and computer intrusions
- 97.2. "False flag" operations – as an extension of the above, where part of the aim is that activity, if discovered, should be specifically attributed to some-one else
- 97.3. Commercially available remote control software has the capability to make use of cameras and microphones¹⁰⁸. There is thus the possibility that an authorisation to intrude into a computer also acts as an authorisation to carry out live audio and video eavesdropping – and also make recordings.

98. Social Engineering The aim of the deployment of social engineering tricks is intrusion in which the target unknowingly assists the hacker/investigator. Typically the result of the trick is

¹⁰⁸ See paragraph 24 above.

information in the form of credentials which are then later exploited. It is not clear how far this route is covered by the draft EI CoP. Is it the case that the deception is not EI, but the consequences are? At what stage does a warrant authoriser become engaged?

99. **Computer Attacks** This aspect may be outside the immediate remit of this case before the Tribunal but in considering issues of authorisation and oversight it is also worth considering the situations where attacks are mounted on specific computers and how these are authorised. These are sometime characterised as “takedowns” and “disruptions”. These can be aimed at state enemies, terrorist groups and international cybercriminals. Are these situations covered under “Equipment Interference” or more generally under, for example, ss 5-7 Intelligence Services Act, 1994?

Legal and Procedural issues

100. The requirements of the law are a matter for the Tribunal, not me. But there are a number of practical matters which I believe ought to be, but are not currently to my knowledge, reflected in Codes of Practice and guidance offered to those asked to authorise and oversee. None of the comments below should be read as legal submissions but are based on my practical experience of the criminal justice system.

101. The Draft EI Code plainly recognises the need to assess for proportionality (to be exercised by the Secretary of State):

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed interference against what is sought to be achieved;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.¹⁰⁹

102. But the Draft EI makes no reference to any specific CNE situation although parts 2 and 4 cover general criteria and expectations. The problem remains that those who authorise and oversee may not have sufficient knowledge of the range of technologies and their application to be able to make informed and plausible judgements.

103. **What is the function of a Code of Practice?** It might be helpful at this point to reflect on why Codes of Practice exist and their various purposes: these seem to be:

103.1. To provide a level of detail which could not be incorporated in primary legislation but which nevertheless has acquired Parliamentary approval where it has been reviewed

103.2. To provide guidance and interpretation to those who seek authorisation, those who give it, and those who act on authorisations

103.3. To alert investigators and others of limitations to their powers which they need to respect

103.4. To give a basis for post-deployment criticism, including if necessary by Commissioners, Tribunals, Courts, Parliamentary committees

It is surely not simply to provide wide-ranging cover for a large variety of disparate actions which can then be said to be compliant with the code.

104. It is instructive to compare the draft EI CoP with others issued, for example under the Police and Criminal Evidence Act,

¹⁰⁹ Paragraph 2.4 to 2.8

1984¹¹⁰. Code A covers searches of persons, Code B covers searches of premises and seizure of property, Code C deals with the detention, treatment and questioning of suspects. In all instances there is a great deal more detail. If we look at the CoP for Covert Surveillance¹¹¹ we see in Chapter 2 general rules on authorisations and extensive discussion of the differences between directed and intrusive surveillance.

105. **Intercepts and Intrusions** In paragraph 96 above I have already shown that given the vast amount of data that will inevitably be found on an accessed computer and the indiscriminate nature of non-CSP forms of interception, the practicalities of making judgements on necessity, proportionality and limitation of collateral intrusion are considerable. Those making these decisions will need technical advice, separate from that used by investigators. I pick up this issue below at paragraph 115
106. It is extremely difficult to predict what will be found on any given targeted computer. Investigators will undoubtedly have a list of items they hope to find but will have little idea how much material will be irrelevant to their aims but nevertheless be “private” to others.
107. As a result of the various capabilities of remote control software there is a danger that an authority to enter a computer is also an authority to monitor live activity in the computer – and its immediate environment. The current draft EI CoP does not make explicit provision for this.
108. Any intrusion into a computer is likely to result in a change to the contents of the device unless the most stringent precautions are taken. The precautions usually followed by law enforcement in imaging disks – the use of write-protect devices – may not be

¹¹⁰ Current codes accessible from <https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-police-codes-of-practice>

¹¹¹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interference_web__2_.pdf

operationally feasible in a covert intelligence exercise. The risk, if there is an eventual criminal prosecution, is of potential defence accusations of evidence tampering. This risk can be partly mitigated if there is a very full log of all investigatory activity – but the Agencies may not wish to reveal such a log on the basis that it may weaken future investigations by revealing methods.

109. It is highly likely that computers seized from suspects and where those computers have been subject to CNE will want to be tendered in evidence in any subsequent criminal proceedings given the quantity of material likely to assist¹¹². The position is thus different from that with interception evidence, currently rendered inadmissible under s 17 RIPA 2000. Whereas a prosecution may be able to proceed without referring to an interception – because other evidence is available – it seems highly unlikely that substantial cases can be prosecuted without reliance on the contents of computers.

110. The intrusion would ordinarily have to be disclosed under Criminal Procedure and Investigations Acts 1996 and 2003. “The test is an objective one. To comply, the prosecutor must disclose to the accused any prosecution material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused, save to the extent that the court, on application by the prosecutor, orders it is not in the public interest to disclose it.”¹¹³ Following the amendment of s 10 Computer Misuse Act 1990 (“CMA”) by s 44 Serious Crime Act 2015 it seems highly likely that defence lawyers will routinely enquire whether powers under s 10 CMA have been deployed, and with what results. One benefit could be to alert a judge if it was thought an *ex parte* application might be made. If a prosecution decision were made to NCND or claim Public Interest Immunity in respect of Agency activity, then defence lawyers are likely to argue

¹¹² There is reference to this in the draft EI CoP at paragraph 6.3

¹¹³ http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/disclosure_manual_chapter_11/

for judicial discretion to exclude the entire related computer evidence, under s 78 PACE 1984.

111. There is a potential clash between a EI CoP requirement to dispose of material when it is no longer needed and the possibility that material needs to be retained for possible future criminal proceedings, including defence arguments that material acquired but subsequently destroyed might have altered the course of a criminal trial (s 78 PACE again).¹¹⁴

Oversight and Audit Trails

112. Oversight, whether by commissioners, the ISC, judges (perhaps under future legislation as suggested by David Anderson QC) or indeed ministers is impossible without historic records. In the authorisation / granting phase those making the judgements may want to know what has happened prior to the request being made. Evidence to support necessity, proportionality and limitation of collateral intrusion may be necessary. I have personal detailed knowledge of what is involved in law enforcement processes for seeking access to communications data.

113. In the case of post-event reviews – to cover the process of granting the authorisation and all the events in its execution and exploitation – detailed logs are surely essential. These logs will need to include: a detailed contemporaneous log of manual notes of decisions and actions generated by authorised staff, computer activity logging, and screen capture software on all devices used by investigators to carry out CNE operations¹¹⁵. I believe that these procedures are followed by police Covert Internet Investigators (CIIs).

¹¹⁴ The Draft EI CoP addresses these at paras 6.10 and 6.5

¹¹⁵ In the “open” world a product such as Camtasia can do this. <https://www.techsmith.com/camtasia.html>

114. There are indications that GCHQ does have some internal auditing facilities¹¹⁶ but without more detailed examination of the reports against the activities it is difficult to assess whether these arrangements provide sufficient detail for any oversight team. I exhibit two documents as PMS/29 and PMS/30.
115. Any oversight team will need to have its own independent technical resource with knowledge of the law, investigative practice and the capabilities of the various CNE technologies. The need will be at its greatest where the techniques are multi-stage, where the amounts of collateral intrusion are not obvious, and where an investigation includes the use of data mining software to integrate several independent streams of evidence. It must be recognised, however, that recruiting such a technical resource may not be easy, as the obvious source of expertise, and with the appropriate security clearance, is former staffers of GCHQ and some of its contractors.

I am happy to provide the Tribunal with further information, if so requested, and to appear before it.



Peter Sommer

30 September 2015

¹¹⁶ <https://theintercept.com/document/2015/09/25/hra-auditing/>;
<https://theintercept.com/document/2015/09/25/sensitive-targeting-authorisation>

IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT 14/85/CH
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL Case No. IPT 14/120-
126/CH

BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Respondents

WITNESS STATEMENT OF ERIC KING

I, ERIC KING, Deputy Director of Privacy International of 62 Britton Street,
London EC1M 5UY, SAY AS FOLLOWS:

1. I am the Deputy Director of Privacy International. I am authorised to make this statement on behalf of Privacy International.
2. I have worked on issues related to communications surveillance at Privacy International since 2011. My areas of interest and expertise are signals

intelligence, surveillance technologies and communications surveillance practices. I regularly speak at academic conferences, with government policy makers, and to international media.

3. The contents of this statement are true to the best of my knowledge, information and belief, and are the product of discussion and consultation with other experts. Where I rely on other sources, I have endeavoured to identify the source.
4. In this statement I will address, in turn, the following matters:
 - a. **Computer Network Exploitation: Introduction**
 - b. **The Five Eyes**
 - c. **What malware can do against an individual device**
 - i. *Activating sensors*
 - ii. *Obtaining stored data from devices*
 - iii. *CNE as a alternative to intercept*
 - iv. *Other CNE capabilities*
 - d. **What malware can do against a server or network**
 - i. *CNE to redirect and capture communications*
 - ii. *CNE to facilitate deployment of further CNE attacks*
 - iii. *CNE for capturing bulk data*
 - iv. *Other CNE capabilities*
 - e. **How malware is deployed**
 - f. **Additional harmful consequences of CNE**
 - i. *Stockpiling of zero days*
 - ii. *Affirmatively weakening security protections*
 - iii. *Influencing technical standards*
 - iv. *"Supply chain enabling, exploitation and intervention"*
 - v. *Faking security updates*
 - vi. *CNE technical failures*
 - vii. *Inability to remove CNE malware*
 - g. **Targets not of national security interest**
 - i. *Targeting companies to enable CNE missions*
 - ii. *Targeting suspicionless people with CNE as a means to an end*

- iii. *Using suspicionless people as "data mules" for CNE*
- iv. *Increasing the likelihood of suspicionless people being attacked by CNE*

h. The scale of CNE deployments

Computer Network Exploitation: Introduction

5. Smartphones, laptops and electronic devices have changed how we communicate and interact with others, express ourselves, and record and remember our thoughts and experiences. These devices have become prime targets for GCHQ and the NSA.
6. These intelligence agencies have developed hacking techniques they call “Computer Network Exploitation” (CNE) or “Active Signals Intelligence” (Active SIGINT), which, NSA documents explain, “offers a more aggressive approach to SIGINT. We retrieve data through intervention in our targets’ computers or network devices. Extract data from machine.”¹ With these capabilities to infect devices with intrusive malware,² GCHQ hopes to be able to “exploit any phone, anywhere, any time.”³ A GCHQ document explains: “if it’s on the phone, we can get it.”⁴
7. With the February 2015 publication of the *Equipment Interference Code of Practice*⁵, CNE became an avowed technique in the United Kingdom. However, Five Eyes members have employed the term CNE since at least 1999⁶.
8. Having now avowed the use of CNE, the Intelligence and Security Committee has reported that “a significant number” of GCHQ’s intelligence reports contain

¹ Intelligent Command and Control (15 March 2014) [Online]. Available from:

https://www.eff.org/files/2014/04/09/20140315-intercept-turbine_intelligence_command_and_control.pdf [Accessed 1 October 2015]

² Malware is specialized software that allows whoever deploys it to take control of or extract information from a target device. This is usually accomplished by circumventing any security software or other protections present on the device.

³ Borger, J. and Hopkins, N. (1 August 2013) Exclusive: NSA pays £100m in secret funding for GCHQ. *The Guardian* [Online]. Available from: <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden> [Accessed 1 October 2015]

⁴ Capability - iPhone (28 January 2014) [Online]. Available from: <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data/img-3> [Accessed 1 October 2015]

⁵ United Kingdom, Home Office (6 February 2015) *Equipment Interference Code of Practice*. [Online]. Available from:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf [Accessed 28 September 2015]

⁶ iPhone Location Services (9 September 2013) [Online]. Available from:

<https://www.eff.org/files/2013/11/15/20130909-spiegel-smartphones.pdf> [Accessed 28 September 2015]

information derived from the technique.⁷ GCHQ and the other UK intelligence agencies may deploy CNE against “computers, servers, routers, laptops, mobile phones and other devices.”⁸

9. One NSA presentation published by *Der Spiegel* highlights just how powerful this capability is with reference to George Orwell’s *1984*. The author of the NSA document asks, “Who knew in 1984 that this [Apple co-founder Steve Jobs] would be Big Brother...and the zombies would be paying customers?”⁹
10. As I will present in more detail below, CNE gives intelligence agencies access to the most personal and sensitive information about an individual’s life – information which can directly or indirectly reveal an individual’s location, age, gender, marital status, finances, health details, ethnicity, sexual orientation, education, family relationships, private communications and, potentially, their most intimate thoughts. Furthermore, the logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies to conduct real-time surveillance, while access to stored data enables analysis of a user’s movements for a lengthy period prior to the search.
11. CNE is thus far more than an alternative to intercept capabilities or a supporting technique for traditional human intelligence (HUMINT). It is the most powerful and intrusive capability GCHQ possesses, and its deployment has revolutionised how GCHQ operates.

The Five Eyes

12. It is well documented that the NSA and GCHQ co-operate very closely, in particular through the Five Eyes alliance, which also includes the intelligence agencies of Canada, Australia and New Zealand. They have co-operated as a

⁷ Intelligence and Security Committee, Parliament of the United Kingdom (12 March 2015) *Privacy and Security: A modern and transparent legal framework* (hereafter “ISC Report”), at 67. The ISC Report covers the UK intelligence agencies’ “IT Operations” primarily on pages 63-67.

⁸ *Ibid.* at 14n.13.

⁹ NSA slides on smartphones (9 September 2013) [Online]. Available from: <https://www.eff.org/files/2013/11/15/20130909-spiegel-smartphones.pdf> [Accessed 28 September 2015]

signals intelligence alliance for almost 70 years. While the alliance was founded when the agencies only carried out passive SIGINT collection, their co-operation has extended to other capabilities as they have become possible, including CNE.

13. **The Five Eyes share the development of CNE capability.** There are specialised Five Eyes teams, such as the Network Tradecraft Advancement Team¹⁰, that seek to improve CNE capability. Security researchers have identified core malware development libraries of software that have been collectively created and used by the USA, the UK, Canada, Australia and New Zealand. These libraries serve as a foundation to allow each country to develop its own malware from a common basis, as well as shared Five Eyes malware.¹¹ Canadian Communications Security Establishment (CSE) documents highlight success stories that are a direct result of British GCHQ analysts identifying new ways to target mobile phones during an Australian Defense Signals Directorate (DSD) workshop.¹² Indeed, the malware itself is shared property of the Five Eyes, with documents explaining that codenamed programs such as WARRIORPRIDE, a key malware framework, is a “unified framework... [used] across the 5 eyes [sic].”¹³

14. **The Five Eyes work together to deploy CNE capability.** *The Intercept* has reported that the NSA and GCHQ have targeted anti-virus and other security companies such as Kaspersky Lab.¹⁴ *The Globe and Mail* has also reported that

¹⁰ NSA GCHQ CSEC Network Tradecraft Advancement [Online] (4 December 2014) [Online]. Available from: https://www.eff.org/files/2014/12/16/20141204-intercept-nsa_gchq_csec_network_tradecraft_advancement.pdf [Accessed 28 September 2015]

¹¹ Guarnieri, C. (27 January 2015) 'Everything we know of NSA and Five Eyes malware' [Online]. Available from: <https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html> [Accessed 28 September 2015]

¹² Synergising Network Analysis Tradecraft (21 May 2015) [Online]. Available from: https://www.eff.org/files/2015/06/30/20150521-cbc-synergising_network_analysis_tradecraft.pdf [Accessed 28 September 2015]

¹³ CSEC Document on the Handling of Existing Trojans When Trojanizing Computers (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/23/20150117-speigel-csec_document_on_the_handling_of_existing_trojans_when_trojanizing_computers.pdf [Accessed 28 September 2015]

¹⁴ Fishman, A. and Marquis-Bore, M. (22 June 2015) Popular Security Software Came Under Relentless NSA And GCHQ Attacks [Online]. *The Intercept*. Available from: <https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/> [Accessed 28 September 2015]

the Canadian CSE and the NSA jointly targeted Brazil's Ministry of Mines and Energy.¹⁵ Even intelligence agencies that are not part of the Five Eyes alliance have been brought in for joint CNE operations, with GCHQ receiving redirected communications traffic from the Swedish National Defence Radio Establishment (FRA), allowing them to inject malware into emails.¹⁶

15. Much of the covert infrastructure to support CNE capability is jointly operated out of Five Eyes bases. NSA documents refer to deploying CNE from RAF "Menwith Hill Station" and "with help from GCHQ".¹⁷ For a period of time, the NSA was seemingly unable to inject malware into users of Google services, with *Der Spiegel* explaining that this "can only be done by Britain's GCHQ intelligence service, which has acquired QUANTUM tools from the NSA."¹⁸
16. The Five Eyes share the data that is collected from many CNE operations, regardless of who initiated it.¹⁹ Documents show that "almost all" of the data from GCHQ CNE operations flows into a Five Eyes joint database, and that "lots" of data from NSA does the same.²⁰
17. Throughout this statement, I will refer to many documents that hold security classification markings "TOP SECRET//REL TO: FVEY", indicating that they were shared with all members of the Five Eyes alliance. While some of the references might be to American NSA documents or to Canadian CSE documents, this statement will make use of such documents to illustrate to the

¹⁵ Freeze, C. and Nolen, S. (7 October 2013) Charges that Canada spied on Brazil unveil CSEC's inner workings [Online], *The Globe and Mail*. Available from:

<http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/> [Accessed 28 September 2015]

¹⁶ XKeyscore Sweden Meeting (12 November 2013) [Online]. Available from:

https://www.eff.org/files/2014/01/02/20131211-svt-xkeyscore_sweden_meeting.pdf [Accessed 28 September 2015]

¹⁷ MHS Leverages XKS for QUANTUM (12 March 2014) [Online]. Available from:

https://www.eff.org/files/2014/04/09/20140312-intercept-mhs_leverages_xkeyscore_for_quantum.pdf [Accessed 28 September 2015]

¹⁸ *Spiegel* staff (29 December 2013) Inside TAO: Documents Reveal Top NSA Hacking Unit, *Der Spiegel* [Online]. Available from: <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html> [Accessed 28 September 2015]

¹⁹ XKeyscore for Counter-CNE (1 July 2015) [Online]. Available from:

https://www.eff.org/files/2015/07/06/20150701-intercept-xks_for_counter_cne.pdf [Accessed 28 September 2015]

²⁰ *Ibid*

Tribunal the types of CNE capabilities being used by the Five Eyes. Due to the high level of operational integration among the Five Eyes members, and the fact that these documents share the "TOP SECRET//REL TO: FVEY" classification markings, I will treat them as relevant regardless of which agency authored the documents.

What malware can do against an individual device

18. When CNE is deployed against an individual's mobile phone or computer, there are few limits on what that malware can do. Unlike bugging or intercept, there is no set way CNE may be used. Instead, it is a capability that can be deployed in any number of configurations to do any number of different things. The Five Eyes have a diverse arsenal of malware tools, each highly sophisticated and customisable for different purposes.

Activating sensors

19. Far from being simply passive storage devices, smartphones are portable sensors that monitor the world around them. Vic Gundotra, Google's Vice President of Social on Android, describes a mobile phone as having "eyes, ears, a skin, and ...[it] knows your location. Eyes, because you never see one that doesn't have a camera. Ears, because they all have microphones. Skin because a lot of these devices are touch screens. And GPS allows you to know your location."²¹
20. Hacking a mobile phone gives governments (or others) total control of features like the camera, microphone and keyboard, which may be utilised, manipulated and turned against the user of the device. Internal GCHQ documents explain that the agency is interested in "[n]ot just collecting voice and SMS and geo-locating phone, but getting intelligence from all the extra functionality that iPhones and BlackBerrys offer."²²

²¹ Gundotra, V. (10 December 2012) Google+ Post [Online]. Available from: <https://plus.google.com/+VicGundotra/posts/f3274job3aN> [Accessed 28 September 2015]

²² Borger, J., Harding, L. and Hopkins, N. (2 August 2013) GCHQ: inside the top-secret world of Britain's biggest spy agency, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden> [Accessed 28 September 2015]

21. This ability to activate features is not limited to mobile phones. One malware implant deployed by the NSA – codenamed UNITEDRAKE – can be used with a variety of “plug-ins” that enable the agency using it to gain total control of an infected computer. For example, an implant plug-in named CAPTIVATEDAUDIENCE is used to hijack a computer’s microphone and record any conversation or audio taking place near the device. Another, GUMFISH, can secretly activate a computer’s webcam and take photographs of whoever is in sight.²³
22. A similar, possibly identical, suite of tools – codenamed WARRIOR PRIDE – is used by GCHQ. This framework includes a range of capabilities: using DREAMY SMURF, GCHQ are able to turn on a mobile phone that is apparently switched off; NOSEY SMURF allows the agency to activate the device’s microphone; and TRACKER SMURF allows the agency to activate the device’s GPS location tracker.²⁴
23. Modules of another piece of Five Eyes malware, Flame, have been analysed by security researchers, who noted the sophistication of many aspects of the malware. In the Flame malware, a screenshot module takes snapshots of whatever is on the screen every 15 seconds when a communication application, such as instant messaging or Outlook, is being used, but decreases this to once every 60 seconds when other, potentially less interesting applications are being used.²⁵
24. To ensure that the presence of malware is not detected, PARANOID SMURF helps the malware to remain hidden on the device.²⁶

²³ Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect ‘Millions’ Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

²⁴ Ball, J. (28 January 2014) Angry Birds and ‘leaky’ phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data> [Accessed 28 September 2015]

²⁵ Zetter, K. (28 May 2012) Meet ‘Flame,’ The Massive Spy Malware Infiltrating Iranian Computers, *Wired* [Online]. Available from: <http://www.wired.com/2012/05/flame/> [Accessed 28 September 2015]

²⁶ Ball, J. (28 January 2014) Angry Birds and ‘leaky’ phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data> [Accessed 28 September 2015]

25. GCHQ is able to record every keystroke pressed on a device using QWERTY, a keylogger plug-in for the WARRIORPRIDE malware framework, designed to collect and exfiltrate all keyboard keys pressed by the victim and record them for later inspection.²⁷ This enables the agency to see everything that the user has typed, including not just the contents of communications and documents, but also any text that was subsequently deleted, and any passwords that the user entered.

Obtaining stored data from devices

26. For an increasing number of people, personal digital devices contain the most private information they store anywhere. Computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, and correspondence. They are also slowly replacing our formal identification documents, and our bank and credit cards. They hold information that may never have been set down or communicated elsewhere.
27. Whatever information is stored on our computers and mobile phones becomes immediately obtainable with CNE. From text messages, emails and phone records, to address books, notes and calendars, as one GCHQ document explains, "if it's on the phone, we can get it."²⁸
- a. *Communications, social networks and contacts:* Whether it's an email, iMessage, Facebook chat or SMS (text message), almost all communications are now sent using either a computer or mobile phone. With CNE, it does not matter what kind of communication is transmitted if a record of this communication is stored on an electronic device, or access to records can be sought via the device – the malware will be able to obtain it. Address books, friends lists, followers –all are there to be exfiltrated and analysed.

²⁷ Malware from the Five Eyes (27 January 2015) [Online]. Available from: <http://www.spiegel.de/media/media-35668.pdf> [Accessed 28 September 2015]

²⁸ Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data> [Accessed 28 September 2015]

- b. *Documents*: Personal and work documents are stored on the storage drives of devices being targeted by CNE. Accessing cloud file storage services (such as Dropbox, Google Drive or Office 365) via our phones or computers means that deploying malware against these devices may result in the entire electronic document history of the target being obtainable. This is very different from intercept of material that a target has chosen to communicate after a warrant has been issued. The collection of data may go back many years.

- c. *Location*: While TRACKER SMURF allows GCHQ to activate the GPS location tracker on a phone to obtain its current location, historical location information can also be discovered by placing malware on a mobile phone. Many popular smart phones store historical location information.²⁹

28. Information that only exists on that device and was never intended to be sent, copied or shared can be obtained via CNE.

CNE as an alternative to intercept

- 29. Information that could otherwise be obtained by intercept is also available. As phone calls are connected, the malware on the device can copy audio from phone calls and transmit it back to GCHQ in real-time. The same is true for emails being sent from a computer, or indeed any other form of communication that can be transmitted from a computer or mobile device.³⁰

- 30. Video chats using Skype or FaceTime can also be captured using CNE and sent back to GCHQ in real-time.³¹

²⁹ Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data> [Accessed 28 September 2015]

³⁰ JTRIG Tools and Techniques (14 July 2014) [Online]. Available from: <https://www.eff.org/files/2014/07/14/jtrigall.pdf> [1 October 2015]

³¹ *Ibid*

31. Other malware tools used by GCHQ include FOGGYBOTTOM, which records logs of internet browsing histories, and GROK, which is used to log keystrokes, allowing the agency to collect login details and passwords for websites and email accounts.³²

Other CNE capabilities

32. Intelligence agencies are interested in obtaining more than just the information from an individual's computer. NSA documents list other goals such as the ability to "manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves."³³ This is unsurprising: once access to an electronic device has been secured, it is as easy to delete material or insert new material as it is to exfiltrate it.
33. A diverse range of malware has been created in order to achieve different objectives, for example preventing someone from gaining access to a certain website, or preventing an individual from downloading a file from the internet. Malware can be employed to corrupt a target's file downloads. Remote control of a computer allows intelligence agencies to send fake messages from the infected device, or plant or delete documents or data on that computer remotely.³⁴ CNE provides a wide range of powerful options.

What malware can do against a server or network

34. Despite this already long list of what intelligence agencies can achieve using malware, these capabilities become more advanced if we consider the deployment of malware against networks of computers.

³² Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

³³ Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 28 September 2015]

³⁴ Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

35. In the words of an NSA analyst, “there are a plethora of things you could do once you get CNE access to a router... suffice it to say, getting access to a router is very good for the actor, and very bad for the victim.”³⁵
36. One team at the NSA – Tailored Access Operations (TAO) – has software templates to break into common brands and models of “routers, switches and firewalls from multiple product vendor lines.”³⁶
37. Targeted systems and networks are often large-scale and sit at the heart of a company’s or a country’s communications infrastructure. The same NSA analyst quoted above (paragraph 35) explains: “I’m not talking about [hacking] your home ADSL router. I’m talking about bigger routers, such as Ciscos/Junipers/Huaweis used by ISPs [internet service providers] for their infrastructure”.³⁷
38. Far from being a capability of last resort for extreme circumstances, it appears this kind of large-scale attack is being deployed regularly against both company and country communications networks. As one document explains “Hacking routers has been good business for us and our 5-eyes [sic] partners for some time.”³⁸

³⁵ Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: <https://www.eff.org/files/2014/04/09/20140320-intercept-targeting-system-administrator-accounts.pdf> [Accessed 28 September 2015]

³⁶ Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 28 September 2015]

³⁷ Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: <https://www.eff.org/files/2014/04/09/20140320-intercept-targeting-system-administrator-accounts.pdf> [Accessed 28 September 2015]

³⁸ Five Eyes Hacking Large Routers (12 March 2014) [Online]. Available from: <https://www.eff.org/files/2014/04/09/20140312-intercept-five-eyes-hacking-large-routers.pdf> [Accessed 28 September 2015]

39. One document reveals that, by deploying CNE against entire mobile phone networks, the NSA are able to automatically exfiltrate phone billing records and the location of everyone connected to that phone network.³⁹
40. As early as 2008, a published GCHQ Intelligence Services Act 1994 warrant referenced the fact that the “[c]apability against Cisco routers developed by this means has allowed a CNE presence on the Pakistan Internet Exchange which affords access to almost any user of the internet inside Pakistan.”⁴⁰

CNE to redirect and capture communications

41. GCHQ is deploying CNE against core communications infrastructure of other countries in order to obtain access to the communications of any user within the target country. This is done to acquire communications that GCHQ would otherwise have had to seek in partnership with the law enforcement or security forces of that country. GCHQ bypasses such partnerships by routing the hacked communications so they flow past a mass surveillance collection point like TEMPORA where they can be processed and analysed.⁴¹
42. Under one CNE programme codenamed GENIE, the NSA reveals a similar system in which they “provide high quality voice collection by delivering implants [meaning malware] that can identify select conversations of interest within a target network and exfiltrate select cuts back to NSA.”⁴² Such techniques in effect steal the processing power of the target’s computer to do the agency’s work for it.

³⁹ Stealthy Techniques Can Crack Some of SIGINT’s Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

⁴⁰ Application for Renewal of Warrant GPW/1160 (22 June 2015) [Online]. Available from: <https://theintercept.com/document/2015/06/22/gchq-warrant-renewal/> [Accessed 28 September 2015]

⁴¹ Guarnieri, C. (27 January 2015) ‘Everything we know of NSA and Five Eyes malware’ [Online]. Available from: <https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html> [Accessed 28 September 2015]

⁴² NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

43. Other documents confirm specific codenamed programs used by the NSA and GCHQ to achieve such redirection. For instance, when deploying malware on “network infrastructure devices” one NSA document explains it can use HAMMERMILL for “targeted copying” which permits the redirection of only targeted communications, not everything that is flowing over the network.⁴³
44. However “targeted copying” is not the limit of the capability that can be achieved with CNE. A program codenamed BRAVENICKEL allows the capture “an entire [communications] link without selection.”⁴⁴
45. GCHQ also engages in bulk redirection, as a 2008 warrant explains: “[o]ur presence on routers likewise allows us to re-route selected traffic across international links towards passive collection systems.”⁴⁵
46. Telecommunications companies are often the targets of these redirection attacks. Just within Germany, several communications have been compromised by GCHQ. Deutsche Telekom AG, which provides mobile phone, internet and landline service to 60 million people in Germany, was hacked by GCHQ.⁴⁶ Likewise, Netcologne, which operates a fiber-optic network and provides telephone and internet services to 400,000 customers, was targeted by GCHQ, as were German satellite operators Stellar, Cetel, and IABG.⁴⁷
47. Redirection via CNE appears to be part of an international Five Eyes strategy. One NSA document explains the agency will continue to develop its redirection capabilities to “more effectively handle the increasing volumes” of data the agency seeks to acquire, as well as to minimize “unnecessary exposure of the

⁴³ Analytic Challenges from Active-Passive Integration. (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/01/23/20150117-speigel-explanation-of-apex-shaping-to-put-exfiltrating-network-traffic-into-patterns-that-allow-plausible-deniability.pdf> [Accessed 1 October 2015]

⁴⁴ Guarneri, C. (27 January 2015) ‘Everything we know of NSA and Five Eyes malware’ [Online]. Available from: <https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html> [Accessed 1 October 2015]

⁴⁵ GCHQ Application for Renewal of Warrant GPW/1160 (22 June 2015) [Online]. Available from: <https://theintercept.com/document/2015/06/22/gchq-warrant-renewal/> [Accessed 1 October 2015]

⁴⁶ Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from:

<https://firstlook.org/theintercept/2014/09/14/nsa-stellar/> [Accessed 1 October 2015]

⁴⁷ Ibid

covert infrastructure.⁴⁸ As evidence of how valuable such redirection programs are perceived to be, the NSA has allocated more than \$650 million for their use in 2013, with the projected budget passing a \$1 billion in 2017.⁴⁹ Such redirection also enables GCHQ to acquire large quantities of intercept without intercepting the content of every communications link.

CNE to facilitate deployment of further CNE attacks

48. Redirecting communications is not the only thing that can be done when CNE is deployed against a network. There are other reasons why GCHQ attacks networks. GCHQ's deployment of CNE against Belgium's largest telecommunications provider, Belgacom, provides a useful example.
49. GCHQ documents explain the attack was "successful"⁵⁰ which in part allowed GCHQ to redirect communications as I describe above. But, the attack against Belgacom was also designed to accomplish something else. The ultimate goal of hacking Belgacom appears to have been to "enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM [man-in-the-middle] operations⁵¹ against targets roaming using Smart Phones."⁵² In other words, GCHQ wanted to use Belgacom's network to launch further CNE operations against phones that used the network.⁵³

⁴⁸ NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt-from-the-secret-nsa-budget-on-computer-network-operations-code-word-genie.pdf> [Accessed 1 October 2015]

⁴⁹ Guarnieri, C. (27 January 2015) 'Everything we know of NSA and Five Eyes malware' [Online]. Available from: <https://nexus.blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html> [Accessed 28 September 2015]

⁵⁰ CNE Access to BELGACOM (13 December 2014) [Online]. Available from: https://www.eff.org/files/2015/01/23/20141214-intercept-gchq_nac_review_april_june_2011.pdf [Accessed 2 October 2015]

⁵¹ A "man in the middle" attack deploys malware without the active participation of the target. The attack interrupts, or gets in the middle of, a request by the target device to access internet content. For instance, a target computer might be requesting to connect to a particular website. The agent will intercept that request, and respond to it, often by impersonating the website. In their response, the agent will send back malware instead of, or sometimes in addition to, the requested content.

⁵² Operation Socialist (24 October 2013) [Online]. Available from: <https://www.eff.org/files/2013/11/15/20130920-spiegel-belgacom.pdf> [Accessed 1 October 2015]

⁵³ Gallagher, R. (13 December 2014) Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, *The Intercept* [Online]. Available from: <https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/> [Accessed 1 October 2015]

50. Documents show that the Five Eyes have dedicated malware for this task, codenamed STRAITBIZARRE.⁵⁴ When deployed, the malware takes control of the target network infrastructure, which can be used to inject malware into other networks, computers or phones.⁵⁵
51. Another GCHQ program, HACIENDA, exists to scan the communications networks of entire countries, looking for vulnerable computers to attack. According to one GCHQ slide from 2009, GCHQ completed scans of 27 different countries and are prepared to do more.⁵⁶ One goal of the scanning is to create what the Five Eyes have dubbed Operational Relay Boxes (ORBs). These are not target computers, but third party computers owned by individuals, companies and governments. Because they are easily vulnerable to exploitation from GCHQ, these ORBs are the initial CNE targets, allowing the agency to control them and use them as relays for further CNE attacks. The ORBs then sit between the attacker and the target, obscuring the true origins of an attack.⁵⁷
52. Not getting caught is part of the operation; an NSA document explains, “[s]ystem logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals.”

CNE for capturing bulk data

53. CNE can also facilitate the acquisition of “bulk data.” Indeed, GCHQ told the Independent Reviewer David Anderson QC that they needed to maintain the “ability to acquire bulk data, including through the use of new techniques, such as CNE.”⁵⁸

⁵⁴ Quantum Shooter SBZ Notes (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-spiegel-quantumshooter-implant-to-remote-control-computers-from-unknown-third-parties.pdf> [Accessed 1 October 2015]

⁵⁵ *Ibid*

⁵⁶ What is HACIENDA? (15 August 2014) [Online]. Available from: <https://www.eff.org/files/2014/08/18/nsa-gchq-csec-hacienda-heise-14-0816.pdf> [Accessed 1 October 2015]

⁵⁷ NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt-from-the-secret-nsa-budget-on-computer-network-operations-code-word-genie.pdf> [Accessed 1 October 2015]

⁵⁸ Anderson, D. - Independent Reviewer of Terrorism Legislation (June 2015) A Question of Trust: Report of the Investigatory Powers Review [Online]. Available from:

54. A series of attacks by the Five Eyes signals intelligence agencies against companies to obtain the encryption keys used secure mobile phone communications demonstrates what can be done.
55. In one CNE operation against a European company, Gemalto, GCHQ sought to obtain the encryption keys used by SIM cards (a small card containing a computer chip which is used in mobile phones to store identifying information and help encrypt communications). Gemalto makes 2 billion SIM cards a year, which are distributed to mobile phone service providers around the world. A GCHQ presentation states the operation was so successful that GCHQ “believe we have their [Gemalto’s] entire network”⁵⁹ allowing the agency to begin “harvesting [data] at scale.”⁶⁰
56. Other Five Eyes partners are deploying similar attacks to obtain data in bulk, including from other SIM card manufactures. The New York Times reported Australia’s signals intelligence agency, DSD, infiltrated an Indonesian mobile phone company and stole nearly 1.8 million encryption keys used to protect communications.⁶¹ The same document also states that GCHQ was preparing similar SIM card theft operations against one of Gemalto’s competitors, Germany-based SIM card giants Giesecke and Devrient.⁶²

<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/TPR-Report-Print-Version.pdf> [Accessed 1 October 2015]

⁵⁹ Begley, J. and Scahill, J. (19 February 2015) The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle, *The Intercept* [Online]. Available from: <https://theintercept.com/2015/02/19/great-sim-heist/> [Accessed 1 October 2015]

⁶⁰ *Ibid*

⁶¹ Poitras, L. and Risen, J. (15 February 2014) Spying by N.S.A. Ally Entangled U.S. Law Firm, *The New York Times* [Online]. Available from: http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0&mtref=undefined [Accessed 1 October 2015]

⁶² Begley, J. and Scahill, J. (19 February 2015) The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle, *The Intercept* [Online]. Available from: <https://theintercept.com/2015/02/19/great-sim-heist/> [Accessed 1 October 2015]

57. Another attack, this time against an unnamed telephone company, allowed Five Eyes agencies to obtain bulk historical phone billing records, which include the time, date and the location of every phone call made on that network.⁶³

Other CNE capabilities

58. One note in a leaked copy of an internal NSA/GCHQ message board highlighted just a few capabilities available when CNE is used against network routers:

"You could add credentials, allowing yourself to log in any time you choose.

You could add/change routing rules

You could set up a packet capture capability [...]

You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels

*You could install a dorked version of the Operating System with whatever functionality you want pre-built in"*⁶⁴

59. By replacing the router's operating system with a "dorked" or altered version, there would be no need to deploy malware again to obtain additional access, as the very operating system of the router would be under your control until it was updated or the malware discovered.
60. While controlling or extracting information from computers and networks is intrusive, intelligence agencies can also do more. To block access to certain websites, they can deploy QUANTUMSKY.⁶⁵ To prevent someone from downloading a certain file from the internet, then they can use QUANTUMCOPPER to corrupt a target's file downloads.⁶⁶

⁶³ Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

⁶⁴ Five Eyes Hacking Large Routers (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-five_eyes_hacking_large_routers.pdf [Accessed 28 September 2015]

⁶⁵ Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

⁶⁶ Ibid

How malware is deployed

61. CNE is most often carried out by remotely accessing the target device. One NSA document explains that “to maximise agility and minimize risk and cost, a targeted system is usually subverted remotely, via existing tools/implants and infrastructure. When remote access is not possible, field operations are undertaken to physically place hardware implants or software modifications into or near targeted systems.”⁶⁷
62. Historically, one of the primary ways GCHQ would send out malware was in bulk, as spam email. It appears that GCHQ was responsible for at least some of the spam email that we all receive. This “bulk spam mission” however was reportedly slowly becoming less viable, resulting in the success rate of infecting a computer becoming less than 1%.⁶⁸
63. Currently, GCHQ appears to prefer a transmission system developed by the NSA codenamed QUANTUM. Indeed, one NSA document reveals “GCHQ uses technique [sic] for 80% of CNE access.”⁶⁹ QUANTUM isn't a new technique; some of its strains, like QUANTUMINSERT, were first created by the NSA in 2005, or QUANTUMSKY in 2004.⁷⁰
64. QUANTUM consists of a variety of methods that allow intelligence agents to take control of target devices. One QUANTUM variation works by “shooting” malware directly into internet traffic that flows through TEMPORA or similar mass surveillance systems. As TEMPORA or similar systems collect and process communications in bulk, the keyword searching conducted under that program can be repurposed for the deployment of CNE too. Based on keywords

⁶⁷ NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt-from-the-secret-nsa-budget-on-computer-network-operations--code-word-genie.pdf> [Accessed 1 October 2015]

⁶⁸ NSA Phishing Tactics and Man in the Middle Attacks (12 March 2014) [Online]. Available from: <https://www.eff.org/files/2014/03/12/20140312-intercept-nsa-phishing-tactics-and-man-in-the-middle-attacks.pdf> [Accessed 1 October 2015]

⁶⁹ Multiple Methods of Quantum (12 March 2014) [Online]. Available from: <https://www.eff.org/files/2014/04/09/20140312-intercept-multiple-methods-of-quantum.pdf> [Accessed 1 October 2015]

⁷⁰ Ibid

within emails collected, QUANTUMTHEORY can be activated, injecting, or “shooting”, malware into the communication in real time in an attempt to exploit the recipient of the email.⁷¹

65. One base in North Yorkshire, RAF Menwith Hill, has been critical in the deployment of QUANTUM attacks. A document shared with the Five Eyes alliance refers to RAF Menwith Hill as being an early tester of QUANTUM when targeting in particular, Yahoo and Hotmail email accounts. Indeed, for a period of time the NSA was unable to deploy QUANTUM to target users of Google services from any other location than the UK.⁷²
66. Another deployment of QUANTUM, codenamed QUANTUMHAND, works by waiting until the target attempts to log into Facebook, at which point GCHQ intercepts the request to log in. Then GCHQ, not Facebook, responds to the request by sending back concealed malware which tricks the victim’s computer into thinking the communication is being sent from the genuine Facebook.⁷³
67. Another option for interfering with a target device is supply chain exploitation, which is discussed in further detail in the paragraphs 92 to 101 of this statement.
68. Five Eyes agencies have also deployed malware to visitors of online forums.⁷⁴ One attack, carried out by the Equation Group which has been linked to the Five Eyes, sent malware to everyone who logged-into a series of web discussion forums. The security company Kaspersky published a detailed description of the operation.⁷⁵ They explained that the malware was sometimes deployed via advertisements on popular web forums used in the Middle East. Everyone who

⁷¹ MHS Leverages XKS for QUANTUM (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-mhs_leverages_xkeyscore_for_quantum.pdf [Accessed 28 September 2015]

⁷² QUANTUMTHEORY Hacking Tactics (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-the_nsa_and_gchqs_quantumtheory_hacking_tactics.pdf [Accessed 1 October 2015]

⁷³ Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect ‘Millions’ Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 1 October 2015]

⁷⁴ Kaspersky Lab (February 2015) Equation Group: Questions and Answers [Online]. Available from: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf [Accessed 1 October 2015]

⁷⁵ Ibid

visited the compromised forum could be infected, although the operation was partially geographically limited. Visitors to the forum from certain countries, including Jordan, Turkey and Egypt, would not be targeted. Once deployed, the malware infects the computer and installs a validator, named DOUBLEFANTASY, which monitors the computer for a period, reporting back to the person controlling it for further instructions. Those instructions may be either to obtain whatever information is desired from the computer, or if the device is not of interest, the operation may be terminated.⁷⁶

69. Another method of deploying malware is known as a “watering hole” attack. Such attacks are usually accomplished by installing custom code on a website that will infect with malware any device that visits that website. For example, the US Federal Bureau of Investigation (FBI) has admitted to deploying such an attack on the servers of the service Freedom Hosting. Each server was turned into a watering hole, and subsequently infected with malware any device that visited the server whether or not that device was of interest to the FBI.⁷⁷

Additional harmful consequences of CNE

70. CNE by its nature exploits weaknesses in software and hardware that is often used by millions of people. One US intelligence official analogised using CNE to a situation in which “[y]ou pry open the window somewhere and leave it so when you come back the owner doesn’t know it’s unlocked, but you can get back in when you want to.”⁷⁸
71. An internal document reveals GCHQ’s desire for the ability to “exploit any phone, anywhere, any time.”⁷⁹ This goal creates perverse incentives, which may

⁷⁶ Ibid

⁷⁷ Poulsen, K. (13 September 2013) FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, *Wired* [Online]. Available from: <http://www.wired.com/2013/09/freedom-hosting-fbi/> [Accessed 1 October 2015]

⁷⁸ Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 28 September 2015]

⁷⁹ Borger, J. and Hopkins, N. (1 August 2013) Exclusive: NSA pays £100m in secret funding for GCHQ, *The Guardian* [Online]. Available from: <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden> [Accessed 1 October 2015]

lead to sacrificing the security of the communications that we all rely on for banking, commerce and other everyday transactions in the name of access for intelligence agencies.

72. As I will describe below, GCHQ and NSA are stockpiling software vulnerabilities, known as zero days. They are also overtly and covertly weakening the security of some hardware and software at its source, influencing security decisions made at technical standards bodies to suit their goals, and undermining trust in critical systems that people around the world rely on for security.

Stockpiling of zero days

73. GCHQ and the Five Eyes use a variety of methods to exploit hardware and software. Many of those methods rely on the use of a vulnerability – a pre-existing error, often called a “bug”, in hardware or software that allows it to be used in a manner that was not intended or anticipated.
74. In the normal course, when researchers and others discover vulnerabilities, they report the vulnerability to the company responsible for the security of the equipment affected. If GCHQ or the Five Eyes discover a vulnerability, however, they have an incentive not to reveal it in order to use it offensively as part of a CNE attack, or to stockpile it for future use. An NSA classification guide states that “technical details concerning specific software vulnerabilities, when not publically known, and [that] are exploited for CNE activities” hold a minimum classification of TOP SECRET.⁸⁰
75. Zero day vulnerabilities get their name from the fact that, when identified, the computer user has had “zero days” to fix them before attackers can exploit the vulnerability.

⁸⁰ NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt-from-the-secret-nsa-budget-on-computer-network-operations-code-word-genie.pdf> [Accessed 1 October 2015]

76. US intelligence officials have acknowledged that governments have become some of the biggest developers and purchasers of information identifying zero days.⁸¹ One NSA budget shows the agency in 2013 set aside \$25.1 million for investment in “resources to maintain and expand the Nation’s CNE capability by additional covert purchases of software vulnerabilities in support of CNE.”⁸²
77. Almost all technology companies have schemes to purchase zero days affecting their systems, with many offering large sums to security researchers who find the vulnerabilities and bring them to the company to fix. While most companies are providing thousands, or even tens of thousands of dollars for particularly important vulnerabilities, the largest publicly acknowledged payment ever made was \$100,000 for a whole class of vulnerabilities affecting Microsoft’s operation system Windows.⁸³
78. Payments offered by governments for vulnerabilities dwarf those given by the companies in both size and scale. The price of zero days is therefore rising, with one security firm that regularly sells zero days to governments now offering \$1 million for a vulnerability that would allow an attacker to break into an iPhone or iPad running Apple’s newly released iOS 9.⁸⁴
79. By purchasing zero days, and using them offensively as part of attacks, GCHQ and the NSA are preventing preventing potentially millions of individuals and companies from being protected.
80. This perverse situation has drawn criticism in the US, from the President’s own Review Group on Intelligence and Communications Technologies. When

⁸¹ Sanger, D. (12 April 2014) Obama Lets NSA Exploit Some Internet Flaws, Officials Say, *The New York Times* [Online]. Available from: http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=1 [Accessed 1 October 2015]

⁸² NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt-from-the-secret-nsa-budget-on-computer-network-operations-code-word-genie.pdf> [Accessed 1 October 2015]

⁸³ Bort, J. (9 October 2013) Microsoft Paid This Man \$100,000 For Finding A Big Security Flaw In Windows 8.1, *Business Insider* [Online]. Available from: <http://www.businessinsider.com/microsoft-pays-100k-for-windows-8-flaw-2013-10?IR=T> [Accessed 1 October 2015]

⁸⁴ Greenberg, A. (21 September 2015) Spy Agency Contractor Puts Out a \$1M Bounty for an iPhone Hack, *Wired* [Online]. Available from: <http://www.wired.com/2015/09/spy-agency-contractor-puts-1m-bounty-iphone-hack/> [Accessed 1 October 2015]

considering the zero day problem, they recommended that “[i]n almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities — ‘patching’ them — strengthens the security of US Government, critical infrastructure, and other computer systems.”⁸⁵

Affirmatively weakening security protections

81. Not satisfied with being able to outspend any competition in the market for vulnerabilities, GCHQ and the NSA have also undertaken to shape the technology marketplace and weaken the development of security technology to suit the agencies’ goals.
82. The NSA’s SIGINT strategy sets out its goals for 2012, which include “[i]nfluenc[ing] the global commercial encryption market through commercial relationships, HUMINT, and second and third party partners.”⁸⁶ Another briefing document sets out how the NSA wants to “[s]hape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities.”⁸⁷
83. These overt and covert efforts to weaken, and make “exploitable”, commonly used technologies undermine computer security for all. Strong encryption is essential for information assurance, data protection, and cyber security, as well as being a critical underpinning for online commerce and international banking.
84. Despite this, a 2010 GCHQ document states, “[f]or the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet

⁸⁵ President’s Review Group on Intelligence and Communications Technologies (12 December 2013) Liberty And Security in a Changing World [Online]. Available from: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [Accessed 1 October 2015]

⁸⁶ SIGINT Strategy (22 November 2013) [Online]. Available from: https://www.eff.org/files/2013/11/25/20131123-nyt-sigint_strategy_feb_2012.pdf [Accessed 1 October 2015]

⁸⁷ The New York Times (5 September 2015) Secret Documents Reveal N.S.A. Campaign Against Encryption [Online]. Available from: <http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html> [Accessed 1 October 2015]

encryption technologies.”⁸⁸ The program “actively engages US and foreign IT industries to covertly influence and/or overtly leverage their commercial products’ designs” including “inserting vulnerabilities into commercial encryption systems.”⁸⁹

85. Another briefing document explains that in 2013, the NSA will “[c]omplete enabling for [redacted] encryption chips used in Virtual Private Networks and Web encryption devices”⁹⁰ meaning that either by working with the manufacturers of the chips to insert back doors or by exploiting a security flaw in the chips’ design, the NSA will be able to break the encryption.⁹¹
86. Virtual Private Networks (VPNs) are important tools that allow individuals and organisations to keep data secure as it is transmitted over the internet. Many businesses use dedicated hardware to encrypt traffic before it is sent using a VPN. Indeed, the guidance provided by the UK Cabinet Office recommends that businesses ensure “device and information exchanges are protected by an appropriately configured VPN.”⁹² By undermining VPNs, the NSA not only makes them vulnerable to exploitation for intelligence agencies, but also by other actors who might discover the weaknesses and exploit them.
87. Certain companies appear to be working with the NSA/GCHQ to ensure their products are “exploitable.” Little is known about which companies are likely to be involved, but one document from the NSA explains that “documents that contain information that implies that commercial companies cooperate with NSA or Second Party partners to render their products exploitable” are to be classified TOP SECRET. Indeed the document goes on to say “exposure of any

⁸⁸ Ball, J., Borger, J. and Greenwald, G. (6 September 2013) Revealed: how US and UK spy agencies defeat internet privacy and security, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> [Accessed 1 October 2015]

⁸⁹ *Ibid*

⁹⁰ The New York Times (5 September 2015) Secret Documents Reveal N.S.A. Campaign Against Encryption [Online]. Available from: <http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html> [Accessed 1 October 2015]

⁹¹ *Ibid*

⁹² United Kingdom Cabinet Office, Department of Business Innovation and Skills (16 January 2015) 10 Steps: Home and Mobile Working [Online]. Available from: <https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets/10-steps-home-and-mobile-working--1> [Accessed 1 October 2015]

company's commercial cryptanalytic relationship with [NSA] even for a company no longer in existence, will damage [NSA's] credibility with current companies who are approached for assistance."⁹³

88. GCHQ has also contributed to the effort to weaken encryption by establishing a HUMINT Operations Team (HOT). HUMINT, short for "human intelligence", refers to information gleaned directly from human sources or undercover agents. This GCHQ team was, according to an internal document, "responsible for identifying, recruiting and running covert agents in the global telecommunications industry."⁹⁴

Influencing technical standards

89. Technical standards are essential for the compatibility and interoperability of technologies as they are developed, produced and used globally.
90. The NSA has internally stated a goal to "influence policies, standards and specifications for commercial public key technologies."⁹⁵ This is not necessarily sinister in and of itself, as it would be expected that the leading US cryptologic agency would be involved in cryptography standards. However, what is concerning is the fact this statement is made within the context of a document setting out the NSA's signals intelligence (SIGINT) enabling goals, aimed at allowing the NSA to ensure commercial systems are "exploitable through SIGINT collection."⁹⁶
91. The NSA has implemented this strategy in at least one instance involving the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC-DRBG) algorithm, which is used to generate random numbers. Random number

⁹³ Classification Guide for SIGINT Material, 1945-1967 (18 June 2014) [Online]. Available from: https://www.eff.org/files/2014/06/23/guidelines_for_the_classification_of_nsa_sigint_details_1945-1967.pdf [Accessed 1 October 2015]

⁹⁴ Ball, J., Borger, J. and Greenwald, G. (6 September 2013) Revealed: how US and UK spy agencies defeat internet privacy and security, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security> [Accessed 1 October 2015]

⁹⁵ Computer Network Operations - SIGINT Enabling (5 September 2013) [Online]. Available from: https://www.eff.org/files/2014/04/09/20130905-guard-sigint_enabling.pdf [Accessed 1 October 2015]

⁹⁶ Ibid

generation is used throughout security systems to create secure keys and for authentication. If the numbers generated are not random but can be predicted, the encryption system itself will be compromised. Dual_EC-DRBG was a standard promulgated by a number of US and international standards bodies. In 2013, however, the New York Times reported that documents in their possession "appear to confirm" that the NSA had inserted a "backdoor" into Dual_EC-DRBG to allow the NSA to decrypt material that used the algorithm.⁹⁷ The US body responsible for the standard subsequently withdrew it and recommended "current users of Dual_EC-DRBG transition to one of the three remaining approved algorithms as quickly as possible."⁹⁸

"Supply chain enabling, exploitation and intervention"

92. In some circumstances, documents show the NSA has undertaken what it calls "supply chain enabling, exploitation, or intervention operations" including "[h]ardware implant enabling, exploitation or operations."⁹⁹

93. One NSA staffer explains the hardware implant enabling process in full: "Here's how it works: shipments of computer network devices (servers, routers, etc.) being delivered to our targets throughout the world are intercepted. Next, they are redirected to a secret location where Tailored Access Operations/Access Operations (AO-S326) employees, with the support of the Remote Operations Center (S321), enable the installation of beacon implants directly into our targets' electronic devices. These devices are then re-packaged and placed back into transit to the original destination. All of this happens with the support of Intelligence Community partners and the technical wizards in TAO."¹⁰⁰

⁹⁷ The New York Times (5 September 2015) Secret Documents Reveal N.S.A. Campaign Against Encryption [Online]. Available from: <http://www.nytimes.com/interactive/2015/09/05/us/documents-reveal-nsa-campaign-against-encryption.html> [Accessed 1 October 2015]

⁹⁸ United States Department of Commerce, National Institute of Standards and Technology (21 April 2014) NIST Removes Cryptography Algorithm from Random Number Generator Recommendations, *NIST Tech Bear* [Online]. Available from: <http://www.nist.gov/itl/csd/sp800-90-042114.cfm>

⁹⁹ Computer Network Exploitation Classification Guide / 2-59 [Online]. Available from: <http://www.spiegel.de/media/media-35656.pdf> [Accessed 2 October 2015]

¹⁰⁰ Gallagher, S. (14 May 2014) Photos of an NSA "upgrade" factory show Cisco router getting implant, *Ars Technica* [Online]. Available from: <http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/> [Accessed 1 October 2015]

94. Interfering with the network hardware supply chain in this way allows the NSA to place controlled backdoors in the “internet backbone”¹⁰¹ and gain access to communications networks, providing potential access to a whole country’s core communication infrastructure used by millions of people.¹⁰² Details of what can be achieved is set out in the earlier ‘what malware can do against a server, or network’ section of this statement.
95. The document that revealed the NSA’s supply chain operations was accompanied by a photograph showing NSA staff unsealing, opening, altering, repackaging, and resealing routing equipment belonging to the US company Cisco.¹⁰³ In response to this photograph, Cisco wrote to President Obama explaining that “we simply cannot operate this way, our customers trust us to be able to deliver to their doorsteps products that meet the highest standards of integrity and security.”¹⁰⁴ Cisco also began shipping equipment to fake addresses in an effort to avoid NSA interdiction.¹⁰⁵
96. Orders for Cisco products fell 18% in the months after the revelation¹⁰⁶ and some estimates suggest US technology companies may lose as much as \$35 billion in revenue as a result of recent revelations regarding intelligence agency activities.¹⁰⁷
97. Documents obtained by Edward Snowden reveal another form of supply chain exploitation, this time targeted at the development of applications (“apps”) for

¹⁰¹ Stealthy Techniques Can Crack Some of SIGINT’s Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

¹⁰² Ibid

¹⁰³ Ibid

¹⁰⁴ Chambers, J.T (15 May 2014) Letter to President Obama [Online]. Available from: http://www.docstoc.com/docs/170154030/Cisco-Chambers-to-POTUS-2014_05_15pdf [Accessed 1 October 2015]

¹⁰⁵ Pauli, D. (18 March 2015) Cisco posts kit to empty houses to dodge NSA chop shops, *The Register* [Online]. Available from: http://www.theregister.co.uk/2015/03/18/want_to_dodge_nsa_supply_chain_taps_ask_cisco_for_a_dead_drop/ [Accessed 1 October 2015]

¹⁰⁶ Gaouette, N. (26 November 2013) NSA Spying Risks \$35 Billion in U.S. Technology Sales, *Bloomberg Business* [Online]. Available from: <http://www.bloomberg.com/news/articles/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales> [Accessed 1 October 2015]

¹⁰⁷ Whittaker, Z. (9 June 2015) US tech giants to “far exceed” \$35 billion loss in NSA fallout, *ZDNet* [Online]. Available from: <http://www.zdnet.com/article/us-tech-companies-to-far-exceed-35-billion-loss-in-nsa-fallout/> [Accessed 1 October 2015]

Apple's iPhone. Researchers at the CIA created a modified version of Apple's software development tool, Xcode, which is used to make apps for the iPhone. The documents explain how if the modified version of Xcode could be surreptitiously distributed to certain developers, then any subsequent apps created by those developers would be built with backdoors already within them.¹⁰⁸ Depending on which developers used the modified Xcode, and how many used their apps, millions of people could be affected. The documents do not say whether the operation was deployed.

98. In China, security researchers recently discovered a modified version of Apple's Xcode software, dubbed XcodeGhost, had been distributed in exactly this way and used by a number of prominent Chinese developers.
99. While it is not known who is responsible for releasing the modified version of Xcode, and there is some scepticism as to whether US authorities carried out the attack due to sloppy code being used in the malware, the damage caused by XcodeGhost is significant. More than 4000 apps were created with the modified Xcode.¹⁰⁹ Apps created with XcodeGhost were reportedly able to obtain usernames and passwords, infect other apps, redirect visits to websites, and steal iCloud passwords and upload them to the attacker's servers without the victim's knowledge.¹¹⁰
100. The infected apps include those used for instant messaging, banking, maps, stock trading, and games. Among the more well-known apps are the instant messenger app WeChat; Didi Chuxing - the most popular taxi app in China; and

¹⁰⁸ Lee, M. (22 September 2015) Apple's App Store got infected with the same type of malware the CIA developed, *The Intercept* [Online]. Available from: <https://theintercept.com/2015/09/22/apples-app-store-infected-type-malware-cia-developed/> [Accessed 1 October 2015]

¹⁰⁹ Pauli, D. (25 September 2015) XcodeGhost-infected apps open gates to malware hijacking, *The Register* [Online]. Available from: http://www.theregister.co.uk/2015/09/25/xcodeghost_mitm_palo_alto/ [Accessed 1 October 2015]

¹¹⁰ Khandelwal, S. (23 September 2015) Apple's Biggest Hack Ever: 4000 Malicious iOS Store Apps Linked to CIA?, *The Hacker News* [Online]. Available from: <http://thehackernews.com/2015/09/ios-malware-cyber-attack.html> [Accessed 1 October 2015]

Railway 12306 - the only official app used for purchasing train tickets in China.¹¹¹ Millions of people will have been affected.

101. Apple have removed the infected apps from the App Store and published instructions for developers to help them identify if they have been infected.¹¹² Some have described the operation as Apple's biggest ever hack.¹¹³

Faking software updates

102. Updating the software on your mobile phone or computer with the latest security patches is an essential practice for individuals and businesses seeking protect themselves against cyber attacks. While these security updates are pushed to computers automatically, they often require action on behalf of the user to be installed, which many users fail to do. Governments around the world are encouraging the download and installation of software updates as a critical cyber security measure. One UK Home Office cyber security education campaign explains, "Software updates contain vital security upgrades which help protect your device from viruses and hackers [...]. While it's easy to hit 'cancel' and go back to what you're doing, the few minutes it takes to download and install the software updates could save you an enormous amount of time and trouble in the long run."¹¹⁴
103. The Five Eyes are exploiting the trust users place in these updates by deploying fake software updates that install malware.
104. The most prominent example of this practice comes from a high profile malware attack, called Flame, reported by the Washington Post to have been

¹¹¹ Xiao, C. (18 September 2015) Malware XcodeGhost Infects 39 iOS Apps, Including WeChat, Affecting Hundreds of Millions of Users [Online]. Available from: <http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/> [Accessed 1 October 2015]

¹¹² Apple (22 September 2015) Validating Your Version of Xcode [Online]. Available from: <https://developer.apple.com/news/?id=09222015a> [Accessed 1 October 2015]

¹¹³ Khandelwal, S. (23 September 2015) Apple's Biggest Hack Ever: 4000 Malicious iOS Store Apps Linked to CIA?, *The Hacker News* [Online]. Available from: <http://thehackernews.com/2015/09/ios-malware-cyber-attack.html> [Accessed 1 October 2015]

¹¹⁴ HM Government, Installing software updates [Online]. Available from: <https://www.cyberstreetwise.com/software-updates> [Accessed 1 October 2015]

jointly developed by the Five Eyes,¹¹⁵ a fact confirmed by subsequent Snowden documents.¹¹⁶ Over the course of six years, security researchers estimate Flame targeted more than 1,000 computers around the world, mostly in the Middle East.¹¹⁷

105. Flame was designed to spread from one infected computer to other machines on the same network. When uninfected computers update themselves, Flame intercepts the request to the Microsoft Update server and instead delivers malware to the machine that is signed with a fake Microsoft certificate.¹¹⁸
106. At the time Flame was deployed, about 900 million Windows computers trusted and relied on security updates from Microsoft Update.¹¹⁹ Once Flame was discovered, the Microsoft certification process was rebuilt, the delivery mechanism for Windows updates was re-architected and a patch was sent out via Microsoft Update in an emergency security package, ten days earlier than the next planned update. Security companies described the loss of trust and confidence in the software update process as "the nightmare scenario."¹²⁰
107. In a recently leaked policy document, the White House admitted and agreed that exploiting companies automatic software update procedures could "call into question the trustworthiness of established software update channels" and might

¹¹⁵ Miller, G. et al (19 June 2012) U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, *The Washington Post* [Online]. Available from:

https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html [Accessed 1 October 2015]

¹¹⁶ Visit Precip: Lobban (30 April 2014) [Online]. Available from:

https://www.eff.org/files/2014/04/30/20140430-intercept-gcbq_visit.pdf [Accessed 1 October 2015]

¹¹⁷ Zetter, K. (2 October 2015) Did the NSA and the UK's Spy Agency Launch a Joint Cyberattack on Iran?, *Wired* [Online]. Available from: <http://www.wired.com/2015/02/uks-spy-agency-partner-nsa-cyberattacks-iran/> [Accessed 1 October 2015]

¹¹⁸ Zetter, K. (6 April 2014) Flame Hijacks Microsoft Update to Spread Malware Disguised As Legit Code, *Wired* [Online]. Available from: <http://www.wired.com/2012/06/flame-microsoft-certificate/> [Accessed 1 October 2015]

¹¹⁹ Microsoft Update and The Nightmare Scenario (4 June 2012) F-Secure Blog [Online]. Available from: <https://www.f-secure.com/weblog/archives/00002377.html> [Accessed 1 October 2015]

¹²⁰ Keizer, G. (7 June 2012) Microsoft's reaction to Flame shows seriousness of 'Holy Grail' hack, *Computer World* [Online]. Available from: <http://www.computerworld.com/article/2504108/cybercrime-hacking/microsoft-s-reaction-to-flame-shows-seriousness-of--holy-grail--hack.html> [Accessed 1 October 2015]

lead some users to opt out of updates, “rendering their devices significantly less secure as time passed and vulnerabilities were discovered but not patched.”¹²¹

CNE technical failures

108. Unlike more traditional SIGINT collection techniques that acquire communications passively, the active intervention of CNE is fraught with difficulties.
109. Occasionally, unintended consequences occur when targeting large scale, core communications infrastructure with CNE. In 2012, it was reported that 92% of the communications networks providing internet connectivity for Syria suddenly were knocked offline.¹²² At the time, this disruption was widely assumed to have been caused by the Syrian government in order to destabilise opposition groups, and was criticised by world leaders.
110. According to Edward Snowden, the NSA, not the Syrian government, caused the disruption. The NSA had been attempting to use CNE to conduct surveillance on the Syrian network when something went wrong with the operation “and the [targeted] router was bricked instead—rendered totally inoperable. [...] The failure of this router caused Syria to suddenly lose all connection to the internet – although the public didn’t know that the US government was responsible.”¹²³
111. Other documents show that the Syria incident is not a one off occurrence. One NSA document refers to a time when all its malware deployments against a

¹²¹ Obama administration draft paper on technical options for the encryption debate (September 2013) [Online]. Available from: <http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/> [Accessed 1 October 2015]

¹²² Shachtman, N. (29 November 2012) Syria Has Just Been Taken Offline, *Wired* [Online]. Available from: <http://www.wired.com/2012/11/syria-offline/> [Accessed 1 October 2015]

¹²³ Ackerman, S. (13 August 2014) Snowden: NSA accidentally caused Syria’s internet blackout in 2012, *The Guardian* [Online]. Available from: <http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war> [Accessed 1 October 2015]

certain type of Cisco router began “experiencing a software bug that causes [the routers] to intermittently drop out.”¹²⁴

112. On other occasions, poor procedures inside Five Eyes agencies mean that structures set up to deploy CNE capability for missions are not properly decommissioned, leaving loose ends causing damage far beyond the time period of the operation.
113. For instance, security researchers were only able to discover the Five Eyes Equation Group malware, described above in paragraph 68, because of mistakes made by the agencies. The NSA’s registration of some of the web domains used by servers in the NSA command and control structure of the Equation Group malware expired, yet the servers were still operating on auto-pilot allowing researchers to register 20 out of the 300 web domains that appeared to be in use, and acquire information about the victims of the malware attack via those domains.¹²⁵
114. Further, some NSA CNE attacks, such as Stuxnet, whose target was Iranian nuclear facilities, have inadvertently spread. Stuxnet eventually appeared on the company Chevron’s computer network. The CIO of Chevron put it plainly: “We’re finding it in our systems and so are other companies [. . .] [s]o now we have to deal with this.”¹²⁶

Inability to remove CNE malware

115. It also appears to be hard to remove malware from computer systems once it has been deployed. For example, when researchers took over the web domains related to the Five Eyes Equation Group malware, as described above in

¹²⁴ NSA Report: Update Software on all Cisco ONS Nodes [Online]. Available from: <https://search.edwardsnowden.com/docs/UpdatesoftwareonallCiscoONSnodes> [Accessed 2 October 2015]

¹²⁵ Goodin, D. (16 February 2015) How “omnipotent” hackers tied to NSA hid for 14 years—and were found at last, *Ars Technica* [Online]. Available from: <http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/> [Accessed 1 October 2015]

¹²⁶ King, R. (9 November 2012) Virus Aimed at Iran Infected Chevron Network, *The Wall Street Journal*. Available from: <http://www.wsj.com/articles/SB10001424127887324894104578107223667421796> [Accessed 1 October 2015]

paragraph 68, they found that despite the fact that the CNE attack occurred over 12 years ago, victim computers around the world were still infected with the malware, with dozens of them continuing to report in from Russia, Iran, China, and India.¹²⁷

116. This problem is likely to get worse as the complexity of the malware being deployed by Five Eyes agencies increases. It is already a stated goal of the NSA to be able to “[d]evelop and deliver capabilities that will allow endpoint implants to persist in target computers/servers through technology upgrades,” with an emphasis “on developing persistent solutions that incorporate stealth techniques.”¹²⁸

Targets not of national security interest

117. With the convergence of communications technologies, the devices, networks, and platforms that are used by the suspicionless public are the same ones that suffer as GCHQ undertakes CNE attacks, not against national security targets, but against law abiding companies, their staff, researchers, and system administrators, who have only one thing in common with each other – they are a “means to an end.”¹²⁹

Targeting companies to enable CNE missions

118. This statement has already described a number of operations undertaken by the Five Eyes agencies against companies that are not engaging in any wrongdoing and are not considered a national security threat. Whether it is the targeting of European telecommunications companies like Deutsche Telekom AG,¹³⁰

¹²⁷ Goodin, D. (16 February 2015) How “omnipotent” hackers tied to NSA hid for 14 years—and were found at last, *Ars Technica* [Online]. Available from: <http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/> [Accessed 1 October 2015]

¹²⁸ NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

¹²⁹ Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140320-intercept-targeting_system_administrator_accounts.pdf [Accessed 28 September 2015]

¹³⁰ Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: <https://firstlook.org/theintercept/2014/09/14/nsa-stellar/> [Accessed 1 October 2015]

Netcologne,¹³¹ and Belgacom¹³²; Satellite operators like Stellar, Cetel, and IABG,¹³³ or companies that facilitate encryption for mobile phones like Gemalto,¹³⁴ Giesecke and Devrient,¹³⁵ there now appears to be a class of companies, often with thousands of employees, and potentially millions of customers, whose involvement in technology means that the Five Eyes intelligence agencies consider them fair game for targeting.

119. When discussing the rationale for targeting one telecommunications company, NSA documents explain that many of its targets communicate using the company's products; "[w]e want to make sure that we know how to exploit these products [. . .] [to] gain access to networks of interest."¹³⁶
120. GCHQ and the NSA have also monitored researchers at anti-virus companies. One NSA slideshow references a program codenamed CAMBERDADA under which malware apparently was sent to various anti-virus companies. The slideshow also lists 23 anti-virus companies from all over the world, stating just two words - "More Targets!"¹³⁷

Targeting suspicionless people with CNE as a means to an end

121. In addition to companies, GCHQ apparently targets entirely suspicionless people, who are not a national security threat, nor are suspected of having committed any crime.

¹³¹ Ibid

¹³² Gallagher, R. (13 December 2014) Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, *The Intercept* [Online]. Available from: <https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/> [Accessed 1 October 2015]

¹³³ Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: <https://firstlook.org/theintercept/2014/09/14/nsa-stellar/> [Accessed 1 October 2015]

¹³⁴ Begley, J. and Scabill, J. (19 February 2015) The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle, *The Intercept* [Online]. Available from: <https://theintercept.com/2015/02/19/great-sim-heist/> [Accessed 1 October 2015]

¹³⁵ Ibid

¹³⁶ Perlroth, N. and Sangder, D.E. (22 March 2014) N.S.A. Breached Chinese Servers Seen as Security Threat, *The New York Times* [Online]. Available from: http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?_r=1 [Accessed 2 October 2015]

¹³⁷ Fishman, A. and Marquis-Bore, M. (22 June 2015) Popular Security Software Came Under Relentless NSA And GCHQ Attacks [Online], *The Intercept*. Available from: <https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/> [Accessed 28 September 2015]

122. In one post to an NSA internal message board, an NSA staffer described deploying CNE against systems administrators (individuals who run and maintain internal computer networks). By hacking a system administrator's computer, the agency can gain covert access to communications that are processed by his or her company whether that is a telecommunications company, an internet service provider or any other company. In noting why system administrators are targeted, the staffer explains that it makes it easier to gain access to the communications of any "government official that happens to be using the network some admin takes care of."¹³⁸
123. The post – entitled "I hunt sys admins" – makes clear that there is a continuous effort to target such individuals, and that intrusive surveillance is acknowledged as not just something to be deployed against terrorists or other national security threats. "Sys admins are a means to an end," the NSA staffer writes.¹³⁹
124. The NSA staffer explains how, in many circumstances, targeting the system administrator is his or her first port of call; "many times, as soon as I see a target show up on a new network, one of my first goals is, can we get CNE access to the admins on that network, in order to get access to the infrastructure that target is using?"¹⁴⁰
125. Both CNE, and other SIGINT capabilities such as interception, are used in tandem to attack system administrators. The post continues, "all of this boils down to getting an admin's webmail/facebook account in order to QUANTUM it and get CNE access to their box [computer]."¹⁴¹
126. Der Spiegel describes how one computer expert working for a data storage company was heavily targeted: "[a] complex graph of his digital life depicts the man's name in red crosshairs and lists his work computers and those he uses

¹³⁸ Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: <https://www.eff.org/files/2014/04/09/20140320-intercept-targeting-system-administrator-accounts.pdf> [Accessed 28 September 2015]

¹³⁹ Ibid

¹⁴⁰ Ibid

¹⁴¹ Ibid

privately ('suspected tablet PC'). His Skype username is listed, as are his Gmail account and his profile on a social networking site. [...] In short, GCHQ knew everything about the man's digital life."¹⁴²

127. In another operation, codenamed AURORAGOLD, the NSA specifically monitored the content of messages sent and received by more than 1,200 email accounts belonging to individuals not considered a national security threat, nor suspected of any criminal wrongdoing, but who were associated with major mobile phone network operators. By intercepting confidential company planning papers, AURORAGOLD helped the NSA deploy CNE against telecommunications companies.¹⁴³
128. GCHQ similarly attacks telecommunications companies by vacuuming up "a large number of unrelated items" from the private communications of targeted employees.¹⁴⁴
129. Suspicionless people other than system administrators are also targeted. One Belgian computer science professor, Jean Jacques Quisquater, had his personal computer targeted and infected with Regin, malware now confirmed to have been developed by GCHQ and NSA. According to Quisquater, he is aware of other computer science professors who have also been targeted by the same attackers.¹⁴⁵ His scientific research is focussed on devising methods for security and cryptography which he publishes in conferences, journals, patents and standards. When he was asked why he felt he was targeted, Quisquater told newspapers, "[m]aybe cryptography research is under surveillance, maybe some

¹⁴² Spiegel staff (11 November 2013) Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers, *Der Spiegel* [Online]. Available from: <http://www.spiegel.de/international/world/gchq-targets-engineers-with-fake-linkedin-pages-a-932821.html> [Accessed 2 October 2015]

¹⁴³ Gallagher, R. (4 December 2014) Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones/> [Accessed 2 October 2015]

¹⁴⁴ Nakashima, E. (19 February 2015) NSA, Britain's GCHQ allegedly seized encryption keys for millions of phones, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/nsa-britains-gchq-allegedly-seized-encryption-keys-for-millions-of-phones/2015/02/19/369cc8b0-b883-11e4-9423-3d0a1ec335c_story.html [Accessed 2 October 2015]

¹⁴⁵ Constantin, L. (3 February 2014) Prominent cryptographers targeted by malware attacks, *PCWorld* [Online]. Available from: <http://www.pcworld.com/article/2093700/prominent-cryptographer-victim-of-malware-attack-related-to-belgacom-breach.html> [Accessed 2 October 2015]

people hope I have some interesting information or contacts or maybe there's another goal we'll never know."¹⁴⁶

Using suspicionless people as "data mules" for CNE

130. When attacking a computer, the infection with malware is only the first stage. The next stage is collecting and transmitting back information from that computer, whether that is documents, account credentials for other computer systems, or audio recorded using the computer's microphone. This is known as exfiltration.
131. In order to hide this exfiltration trail, intelligence agencies of the Five Eyes have justified even greater intrusion on suspicionless people in order to mask the fact they deployed CNE in the first place. These suspicionless individuals are described as "unwitting data mules" in one NSA presentation.¹⁴⁷ Their purpose, the presentation explains, is to act as middlemen, with the malware forcing their computers to act as a go-between for the NSA and the target of the attack. This is done in multiple stages, with sophisticated operations requiring the "need to transfer data and commands over two or more hops," causing a growing web of suspicionless computers to be caught up in the operation.
132. Research by one anti-virus company, Kaspersky, into a sophisticated piece of malware named Regin, which is widely believed to be the work of intelligence agencies of the Five Eyes, highlighted one such technique, explaining how one attack ended up affecting individuals and their computers from three other organisations. In one country 'X', multiple different groups were hacked, including the president's office, a research centre, an educational institution network and a bank. These victims were spread across the country but all interconnected to each other. Each of them had been attacked and infected with versions of the Regin malware, and was then instructed to communicate and pass information with the others. In this way, a peer-to-peer network was

¹⁴⁶ Ibid

¹⁴⁷ Appelbaum, J. et al. (17 January 2015) The Digital Arms Race: NSA Preps America for Future Battle. Spiegel Online [Online]. Available from: <http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html> [Accessed 2 October 2015]

created, allowing the Five Eye attackers to issue commands to the malware targeting the president's office via the bank's network, with the exfiltrated information passing back via the same route.¹⁴⁸

133. According to Kaspersky, it is not likely the research centre, educational institution, or the bank were the true targets of the attack, but instead they were used as cover to ensure the desired infiltration of the president's office stayed in place.

Increasing the likelihood of suspicionsless people being attacked by CNE

134. As individuals and institutions are now being used as middlemen for the exfiltration of data, the likelihood that other foreign intelligence, or criminal actors will target these "unwitting data mules" also increases.¹⁴⁹
135. One NSA document sets out such a scenario. In a CNE attack against one country (country A), they discovered another country (country B) also had malware running on the same computers the NSA was targeting in country A. The NSA withdrew from targeting the original country A machines, and instead followed the trace back to see who country B were using as an "exfil point" outside the country and instead deployed malware against this suspicionless target, obtaining a copy of everything that country B was getting from the computer in country A. This is known as Fourth Party collection.¹⁵⁰

The scale of CNE deployments

136. CNE was once a rarely used capability. This did not stay the case for long. By 2003, the use of CNE had risen dramatically, and with a few hundred NSA staff

¹⁴⁸ Kaspersky Lab's Global Research & Analysis Team (24 November 2014) *Regin: nation-state ownage of GSM networks* [Online]. Available from: <https://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/> [Accessed 1 October 2015]

¹⁴⁹ Fifth Party Access (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-fifth_party_access_-_when_the_targeted_fourth_party_has_someone_under_surveillance_who_puts_others_under_surveillance.pdf [Accessed 1 October 2015]

¹⁵⁰ *Ibid*

conducting on average 20-25 CNE operations a day, rising again to 100 CNE operations a day by the end of 2005.¹⁵¹

137. Since then the Five Eyes have “aggressively scaled”¹⁵² their hacking initiatives, in the past decade computerizing some processes previously handled by humans. One key system codenamed TURBINE now “allow[s] the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually.”
138. Another document confirms the scale of the ambition, stating TURBINE’s goal is to “increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants.”¹⁵³ Developed as part of the Tailored Access Operations unit, the TURBINE system is described in leaked documents as an “intelligent command and control capability” that enables “industrial-scale exploitation.”¹⁵⁴
139. It is unclear how many devices the Five Eyes have interfered with over the years, but some figures are available. Under one NSA program codenamed GENIE, the goal for the end of 2013 was to “increase the number of Endpoint Points-of Presence worldwide to a range of 85,000-96,000”¹⁵⁵ and the number of “Endpoint active accesses to 9,000-10,000.”¹⁵⁶ Elsewhere the Washington Post reported on the LinkedIn profile of one NSA staffer, whose profile

¹⁵¹ Expansion of the Remote Operations Center (ROC) on Endpoint Operations (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/01/23/20150117-speigel-document-about-the-expansion-of-the-remote-operations-center-roc-on-endpoint-operations.pdf> [Accessed 2 October 2015]

¹⁵² Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

¹⁵³ Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

¹⁵⁴ Ibid

¹⁵⁵ NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: <https://www.eff.org/files/2015/02/03/20150117-speigel-excerpt-from-the-secret-nsa-budget-on-computer-network-operations-code-word-genie.pdf> [Accessed 1 October 2015]

¹⁵⁶ Ibid

included the fact that the 14 personnel under his command had undertaken over 54,000 CNE operations.¹⁵⁷

140. In other areas, even small research teams are working out whether they can deploy CNE in bulk, forcing computers to secretly stamp unique identifiers into every internet packet that leaves that machine. These plans to conduct “large scale staining of machines” have already being deployed.¹⁵⁸ Activities like this, that utilize the bulk capabilities of both SIGINT and CNE will likely increase, as one leaked document explains “this is great example of CNE effects enabling passive SIGINT and then this in turn enabling CNE and will hopefully lead the way for future joint projects.”¹⁵⁹
141. Other malware tools such as SECONDDATE can be used both for tailored “surgical” attacks and to launch bulk malware attacks against computers. According to a 2012 presentation, the tactic has “mass exploitation potential for clients passing through network choke points.”¹⁶⁰



Eric King

5th October 2015

¹⁵⁷ Peterson, A. (29 August 2013) The NSA has its own team of elite hackers, *The Washington Post* [Online]. Available from: <https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/> [Accessed 2 October 2015]

¹⁵⁸ Op MULLENIZE (4 October 2014) [Online]. Available from: https://www.eff.org/files/2013/11/25/20131004-wapo-gchq_mullenize.pdf [Accessed 2 October 2015]

¹⁵⁹ Ibid

¹⁶⁰ Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/> [Accessed 28 September 2015]

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

THE RESPONDENTS' RE-RE-AMENDED OPEN RESPONSE

Privacy International and the Greennet Claimants will be referred to below as "the Claimants".

The term "Respondents" is used below to refer to both Respondents in both Claims.

The IPT judgment in the recent Liberty/Privacy proceedings, [2014] UKIPTrib 13_77-H dated 5 December 2014, is referred to in this Response as "the Liberty/Privacy IPT judgment".

INTRODUCTION

1. The two Claims overlap substantially. For convenience, the Respondents are filing a single Open Response to both Claims.

2. This Open Response:
 - (a) Summarises the need for the “neither confirm nor deny” policy, and explains its operation in the present case pp2-3.
 - (b) Addresses the Tribunal’s procedural regime, insofar as is relevant to the present Claims pp3-5.
 - (c) Addresses the complaints made in the proceedings and in particular :
 - (a) sets out the Respondents’ open position on the factual allegations made pp5-8;
 - (b) sets out the relevant domestic legal regime (“the Equipment Interference Regime”) pp8-44;
 - (c) identifies the pure issue of law which is suitable for determination at a public *inter partes* hearing (“a Legal Issues Hearing”) p44; and
 - (d) sets out the Respondents’ position on that pure issue of law, p45-54.
 - (d) Suggests directions for the future management of these two Claims (p54).
3. The Respondents’ overall position is that the Equipment Interference Regime is compatible with Arts 8, 10 and (if it is engaged by the Greennet complaint) Article 1 of the First Protocol to the ECHR. The Claims should therefore be dismissed.

THE “NEITHER CONFIRM NOR DENY” POLICY, AND ITS OPERATION IN THE PRESENT CASE

4. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See *e.g. Attorney General v. Guardian Newspapers Ltd (No.2)* [1990] 1 AC 109, *per Lord Griffiths* at 269F.
5. As a result, the mere fact that the Intelligence Services are carrying out an investigation or operation in relation to say, a terrorist group or hold information on a suspected terrorist will itself be sensitive. If, for example, a hostile individual or group were to become aware that they were the subject of interest by the Intelligence Services, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps publicly reveal, the methods used by the Intelligence Services or the identities of the officers or agents involved. Conversely, if a hostile individual or group were to become aware that they were not the subject of Intelligence Service interest, they would then know that they could engage or

continue to engage in their undesirable activities with increased vigour and increased confidence that they will not be detected.

6. In addition, an appropriate degree of secrecy must be maintained as regards the intelligence-gathering capabilities and techniques of the Intelligence Services (and any gaps in or limits to those capabilities and techniques). If hostile individuals or groups acquire detailed information on such matters then they will be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services will be able successfully to deploy those capabilities and techniques against them.
7. It has thus been the policy of successive UK Governments to neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or hold information on a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques.
8. Further, the "neither confirm nor deny" principle would be rendered nugatory, and national security thereby seriously damaged, if every time that sensitive information were disclosed without authority (*i.e.* "leaked"), or it was alleged that there had been such unauthorised disclosure of such information, the UK Government were then obliged to confirm or deny the veracity of the information in question.
9. It has thus been the policy of successive Governments to adopt a neither confirm nor deny stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the UK Government.¹ That long-standing policy is applied in this Open Response.

THE TRIBUNAL'S PROCEDURAL REGIME²

10. The Tribunal's procedure is governed by ss. 67-69 of RIPA and the Investigatory Powers Tribunal Rules 2000, SI 2000/2665 ("the Rules"), made under s. 69.
11. In §173 of the Procedural Ruling of 22 January 2003 in IPT/01/62 and IPT/01/77 ("the Procedural Ruling") the Tribunal concluded that r. 9(6) of the Rules³ was *ultra vires* the rule-making power in s. 69 of RIPA. Further, the

¹ Such a confirmation would only be given in exceptional circumstances – for example, on the basis either that there were some compelling countervailing public interest in departing from the neither confirm nor deny principle that clearly outweighed the public interest in protecting national security (or on balance promoted the public interest in protecting national security).

² The Tribunal's jurisdiction and remedial powers are addressed below.

³ R. 9(6) provides:

"The Tribunal's proceedings, including any oral hearing, shall be conducted in private."

Tribunal held that:

- (a) "purely legal arguments, conducted for the sole purpose of ascertaining what is the law and not involving the risk of disclosure of sensitive information" should be heard by the Tribunal in public (Procedural Ruling, §172); and
 - (b) the Tribunal's reasons for its ruling on any "pure questions of law" (§195) that are raised at such a hearing may be published without infringing either r. 13 of the Rules or s. 68(4) of RIPA⁴ (Procedural Ruling, §§190-191).
12. It follows that, where necessary, the Tribunal may hold a Legal Issues Hearing to consider any relevant (and disputed) pure issues of law,⁵ and may subsequently publish its rulings (with its reasoning) on such issues.
13. The Tribunal also concluded in the Procedural Ruling that, with the exception of r. 9(6), the Rules are valid and binding (§148). It follows from this conclusion, and from r. 6(2)-(5) of the Rules, that - prior to the determination of a claim⁶ - the Tribunal cannot disclose to a claimant anything that a respondent has decided should only be disclosed to the Tribunal, and similarly cannot order a respondent to make such disclosure itself.
14. The overall effect of the Procedural Ruling is thus that:
- (a) where necessary, the Tribunal first holds a Legal Issues Hearing to determine such relevant pure issues of law as are in dispute between the parties, and publishes its rulings (with reasons) on those pure issues of law;
 - (b) the Tribunal then investigates the claim in closed session; and
 - (c) as necessary,⁷ the Tribunal applies its rulings on the pure issues of law to the facts that it has found following its closed session investigation of the claim.
15. This was the approach taken in the two joined cases which gave rise to the

⁴ The effect of r. 13 and s. 68(4) is in essence that if the claim is dismissed then the Tribunal may only give to the claimant a statement that "no determination has been made in his favour", but that if the claim is upheld then the Tribunal may, subject to r. 6(1), provide a summary of its determination, including any findings of fact.

⁵ As the Tribunal confirmed in the subsequent case of *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH), 26 February 2008, at §5, the pure issues of law can as necessary be considered on the basis of hypothetical facts.

⁶ As noted in footnote 5 above, the Tribunal has power - subject to r. 6(1) - to provide a summary of its determination, including any findings of fact, in the event that the overall claim is upheld.

⁷ Following its investigation the Tribunal may e.g. find that the respondents have not in fact undertaken any activities in relation to a claimant, with the result that the claim will be dismissed without the need to apply the rulings on the pure issues of law to any specific factual findings.

Procedural Ruling. Following the Procedural Ruling, the two cases were separated and disputed pure issues of law were identified and determined following Legal Issues Hearings (the ruling on the pure issues of law in IPT/01/77 of 9 December 2004 is considered below). Each claim was then finally determined following the Tribunal's investigation of the cases in closed session. This was similarly the approach taken in *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH).⁸

16. The European Court of Human Rights ("the ECtHR") unanimously upheld the Tribunal's procedural regime as summarised above in *Kennedy v. UK* (2011) 52 EHRR 4, at §§184-191. (*Kennedy* arose out of one of the domestic cases that gave rise to the Procedural Ruling, namely IPT/01/62.)
17. In the Respondents' submission therefore, the approach set out in §14 above is the one prescribed in the Rules, is tailored to the subject matter of the matters falling within the Tribunal's jurisdiction, has been expressly accepted as fair and compatible with the ECHR by the ECtHR; and should be followed by the Tribunal in the present Claims.
18. In these proceedings the Claimants seek a public hearing of their complaints (see §10 of Privacy's Grounds and §12 of the Greenet Grounds). It is asserted that documents which have been released into the public domain regarding the alleged technical capabilities and activities of GCHQ mean that there is no good reason to uphold the NCND policy. However, this approach fails to appreciate the ordinary operation of the "neither confirm nor deny" policy in the case of alleged leaks (as set out above). The long-standing general policy is clear: the "neither confirm nor deny" stance is maintained.
19. The Respondents are filing a Closed Response with this Open Response. For the avoidance of doubt, the Respondents' position, with respect to the Tribunal, is that in the light of r. 6 of the Rules, the Procedural Ruling and *Kennedy*, nothing in the Closed Response can be disclosed to the Claimants without the Respondents' consent.

Formatted: Fc

THE RESPONDENT'S OPEN POSITION ON THE FACTUAL ALLEGATIONS

Computer Network Exploitation ('CNE')

20. The allegations made in both claims concern activities known by a number of terms, including "Computer Network Exploitation" or 'CNE'. CNE is a set of techniques through which an individual or organisation gains covert and remote access to equipment (including both networked and mobile computer devices) typically with a view to obtaining information from it.

⁸ There is a class of Tribunal cases that have not proceeded in this way (see e.g. *Paton v. Poole Borough Council*, IPT/09/01-05/C, determination of 29 July 2010). But that is because, in these cases, the respondents have decided that the entirety of their factual case can be dealt with in open session, with the result that the Legal Issues Hearing becomes in effect indistinguishable from a substantive hearing on all disputed matters. Where, however, a respondent decides that any part of its factual case is closed, then the approach in §19 applies.

21. CNE operations vary in complexity. At the lower end of the scale, an individual may use someone's login credentials to gain access to information. More complex operations may involve exploiting vulnerabilities in software in order to gain control of devices or networks to remotely extract information, monitor the user of the device or take control of the device or network. These types of operations can be carried out illegally by hackers or criminals. In limited and carefully controlled circumstances, and for legitimate purposes, these types of operations may also be carried out lawfully by certain public authorities.
22. As with interception, there are a range of circumstances in which the Intelligence Services may be required to conduct this type of activity. CNE can be a critical tool in investigations into the full range of threats to the UK from terrorism, serious and organised crime and other national security threats. For example, CNE is used to secure valuable intelligence to enable the State to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.
23. CNE operations may enable the Intelligence Services to obtain communications and data of individuals who are engaged in activities which are criminal or harmful to national security in circumstances where it may otherwise be difficult or impossible to so obtain them. Such circumstances may arise where, for example:
 - (a) the wanted communications are not in the course of their transmission and cannot therefore be intercepted;
 - (b) there is no communications service provider on whom a warrant can be served to acquire particular communications; or
 - (c) a more comprehensive set of the target's communications or data of intelligence interest is required than can be obtained through other means.

Response to the specific factual allegations in the Grounds of Complaint

24. In its Grounds of Complaint Privacy International alleges, *inter alia*, that GCHQ is involved in the infection of individuals' computers and mobile devices "on a widespread scale"⁹ and in a way which "appears to be indiscriminate in nature"¹⁰ to gain access either to the functions of the devices (eg. activating a camera or microphone without the user's consent) or to obtain stored data. These allegations are made following alleged disclosures made by the former NSA Contractor Edward Snowden (see §§11-18 of the Privacy Grounds).
25. In their Grounds of Complaint the Greennet Claimants allege, *inter alia*, that GCHQ has targeted internet and service communications providers ('ISPs') in order to compromise and gain unauthorised access to their network infrastructures in pursuit of "mass surveillance activities". It is alleged that

⁹ See §3 of the Privacy Grounds

¹⁰ See §8 of the Privacy Grounds

there has been manipulation of the ISP's property and unauthorised changes made to its assets and infrastructure, together with surveillance of the ISP's employees and customers respectively (see §55 of the Greenet Grounds). The claims are said to arise out of reports by the German magazine *Der Spiegel* which were also said to arise from alleged disclosures made by Edward Snowden (see §§3-5 and §§13-26 of the Greenet Grounds).

26. The Respondents neither confirm nor deny all of the specific factual claims relating to the alleged specific technical capabilities and/or conduct of GCHQ as set out in the complaints. Further, and for the avoidance of doubt, the Respondents neither confirm nor deny whether there has been any interference with the Claimants' property (whether as alleged in the complaints or otherwise) or that of their employees/clients/customers, and/or whether such interference led to the consideration or examination of any of the Claimants' information or data and/or the information or data of their employees/clients/customers.
27. It is noted that the Claimants make very extreme factual allegations about the scope, scale and nature of GCHQ's activities in these proceedings. For example Privacy asserts that GCHQ's activity "*appears to be indiscriminate in nature*"¹¹ and that there has been intrusion into "*millions*" of devices which is disproportionate to any legitimate aim¹². Similarly extreme allegations are also made by the Greenet Claimants, including that GCHQ has engaged in "*mass surveillance activities*"¹³; that its activities are "*indiscriminate*" in nature¹⁴ and amount to "*one of the most intrusive forms of surveillance any government has ever conducted*"¹⁵.
28. No assumption can or should be made as to the truth of any of the Claimants' assertions about the intelligence gathering activities of GCHQ. As noted by the Tribunal in the *Liberty/Privacy* judgment "*the indiscriminate trawling for information...whether mass or bulk or otherwise, would be unlawful, as would be the seeking, obtaining or retention of material which is unnecessary or disproportionate*" (see §160(iii)). Thus, whilst the specific factual allegations which are made in these proceedings are neither confirmed nor denied for the reasons set out above, it is denied that GCHQ is engaged in any unlawful and indiscriminate mass surveillance activities. Such activities are clearly precluded by the clear statutory regime which governs GCHQ's activities as set out in detail below.
29. The Respondents nevertheless accept that the Claimants may challenge the general Art. 8-compatibility of the Equipment Interference Regime on the basis that their property/equipment might in principle have been interfered with and that at least some of their data/information may have been considered or examined.
30. As to Article 10 ECHR, in the light of *Österreichische Vereinigung zur Erhaltung*

¹¹ §8 of the Privacy Grounds

¹² §51 of the Privacy Grounds

¹³ §3 of the Greenet Grounds

¹⁴ §10 of the Greenet Grounds

¹⁵ §61(a) of the Greenet Grounds

v. Austria, Appl. No. 39534/07, 28 November 2013, the Respondents accept that, in the present context, non-governmental organisations (such as Privacy International) engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press. In principle, therefore, any interference with Privacy's communications or communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

31. However the Greennet Claimants cannot claim to be victims of any Art. 10 interferences. They are not journalists, news organisations or a species of NGO which is entitled to claim the protection of Article 10 ECHR (see HMG's skeleton in *Liberty/Privacy* dated 3 July 2014 at §§56-59).
32. Further and in any event Article 10 adds nothing to the analysis under Article 8 ECHR – see §147 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5 and see also §12 and §149 of the *Liberty/Privacy* judgment.
33. As to Article 1 of the First Protocol ('A1P1'), this is relied upon by the Greennet Claimants, although it is noted that they advance no evidence in support of the contention that (1) they have suffered any damage or other material alteration of their property, or (2) there has been any damage or detriment to their commercial relationships or loss of goodwill within the meaning discussed in the A1P1 case law (see eg. *R (New London College Ltd) v Secretary of State for the Home Department* [2012] EWCA Civ 51 at §§83-98) (see §37(d) of the Greennet Grounds). This claim therefore appears to be entirely speculative in nature and, in absence of some evidential basis for the alleged interference with their A1P1 rights, including proof of loss and/or damage, should be dismissed. Further and in any event this claim adds nothing to the analysis under Art. 8 ECHR.

THE EQUIPMENT INTERFERENCE REGIME

34. The Equipment Interference Regime which is relevant to the activities of GCHQ principally derives from the following statutes:
 - (a) the Intelligence Services Act 1994 ("the ISA"), (as read with the Counter-Terrorism Act 2008 ("the CTA") and the Computer Misuse Act 1990 ("the CMA"));
 - (b) the Human Rights Act 1998 ("the HRA");
 - (c) the Data Protection Act 1998 ("the DPA"); and
 - (d) the Official Secrets Act 1989 ("the OSA").
35. In addition, the draft Equipment Interference Code of Practice dated February 2015 ('the EI Code') is relevant to the regime as regards the scope of any powers to interfere with property and equipment, as are GCHQ's

internal arrangements in relation to CNE activities (see §§99B-99ZS below).

The ISA (read with the CTA and the CMA)

GCHQ functions

36. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ..."

37. By s. 3(2) of the ISA, these functions are only exercisable:

*"(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
(c) in support of the prevention or detection of serious crime."*

38. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

Disclosure of information

39. By s. 19(5) of the CTA, information obtained by GCHQ for the purposes of any of its functions *"may be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings."*

40. Thus, specific statutory limits are imposed on the information that GCHQ can obtain, and on the information that it can disclose. In addition, the term "information" is a very broad one, and is capable of covering e.g. both communications and communications data.

41. By s. 19(2) of the CTA:

"Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions."

Computer Misuse Act ('CMA')

41A. The Computer Misuse Act 1990 (CMA) came into force on 29 June 1990. It was amended on 3 May 2015 as a result of changes introduced by the Serious Crime Act 2015.

42. By s.1(1) of the CMA:

"(1) A person is guilty of an offence if –
(a) he causes a computer to perform any function with intent to secure access to any program or data¹⁶ held in any computer;
(b) the access he intends to secure, is unauthorised¹⁷; and
(c) he knows at the time when he causes the computer to perform the function that that is the case."

43. Although "computer" is not defined in the CMA, in the context of s.69 of the Police and Criminal Evidence Act 1984 (PACE), the term has been held to mean "a device for storing, processing and retrieving information" (see *DPP v McKeown* [1997] 1 WLR 295 at 302).

44. By s.3 of the CMA it is also an offence to do any unauthorised act¹⁸ in relation

¹⁶ Section 17 of the CMA provides, *inter alia*, that:

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he –

- (a) alters or erases the program or data;*
- (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;*
- (c) uses it; or*
- (d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);*

and references to access to a program or data (and to an intent to secure such access [or to enable such access to be secured] 1) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform –

- (a) causes the program to be executed; or*
- (b) is itself a function of the program.*

(4) For the purposes of subsection (2)(d) above –

- (a) a program is output if the instructions of which it consists are output; and*
- (b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial. ...*

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

¹⁷ By section 17(5) of the CMA - "Access of any kind by any person to any program or data held in a computer is unauthorised if – (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled" (NB. this subsection is subject to section 10 which contains a saving in respect of certain law enforcement powers).

¹⁸ By s. 17(8) of the CMA - An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done) – (a) is not himself a person who has responsibility for the computer

to a computer, if, at the time that he does the act the person knows that it is unauthorised (s. 3(1)) and either (1) the intention is to impair the operation of any computer; to prevent or hinder access to any program or data held in any computer; to impair the operation of any such program or the reliability of any such data (s. 3(2)(a)-(c)), or (2) the person is reckless as to whether the act will do any of those things s. 3(3)).

45. Section 4 of the CMA sets out the territorial scope of, *inter alia*, offences under s. 1 and s. 3 of the CMA. In particular this makes clear that it is immaterial for the purposes of any offence under s.1 or s.3 of the CMA (a) whether any act or other event, proof of which is required for conviction of the offence, occurred in England or Wales; or (b) whether the accused was in England or Wales at the time of any such act or event. Save in respect of certain offences (i.e. under s. 2 of the CMA), at least one significant link with domestic jurisdiction must exist in the circumstances of the case for an offence to be committed. The tests as to whether there is a significant link with domestic jurisdiction are set out in section 5 of the CMA.

46. Summary conviction under the CMA in respect of offences under s. 1 and s. 3 may lead to imprisonment for a term not exceeding 12 months or a fine (see s. 1(3)(a) and s. 3(6)(a) CMA). Any conviction on indictment may lead to imprisonment for a term not exceeding 2 years or to a fine, or both, in respect of a s. 1 offence (see s. 1(3)(c)) and for a term not exceeding 10 years, or to a fine, or both in respect of a s. 3 offence (see s. 3(6)(c) CMA).

46A. Section 10 of the CMA (prior to amendments introduced on 3 May 2015) provided as follows:

*"Saving for certain law enforcement powers
Section 1(1) above has effect without prejudice to the operation –
(a) In England and Wales of any enactment relating to powers of inspection,
search or seizure."*

46B. As set out at §37A of the Amended Grounds in the Privacy Complaint, on 3 May 2015 the CMA was amended. Those amendments (which it is accepted are not retrospective) included, *inter alia*:

a) Changes to the test under section 5 as to when a significant link with domestic jurisdiction is established in respect of offences under, *inter alia*, sections 1 and 3 of the CMA;

b) Changes to section 10 of the CMA, which now provides *inter alia*:

*"Savings
Sections 1 to 3A have effect without prejudice to the operation –
(a) in England and Wales of any enactment relating to powers of inspection,
search or seizure or of any other enactment by virtue of which the conduct in*

and is entitled to determine whether the act may be done; and (b) does not have consent to the act from any such person. In this subsection "act" includes a series of acts.

Authorisation for equipment interference

s.5. warrants

47. By s. 5 of the ISA the Intelligence Services, including GCHQ, can apply for a warrant which provides specific legal authorisation for property interferences by them. Thus by s5(1) of the ISA:

"(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.

48. In relation to GCHQ, pursuant to s.5(2)(a)-(c) of the ISA the Secretary of State can only issue a warrant under s.5 following an application by GCHQ if he/she is satisfied that:

(a) it is **necessary** for the action to be taken for the purpose of assisting GCHQ in carrying out its statutory functions under s. 3(1)(a) of the ISA;

(b) the taking of the action is **proportionate** to what the action seeks to achieve; and

(c) **satisfactory arrangements** are in force under section 4(2)(a) of the ISA with respect to the disclosure of information by GCHQ obtained by virtue of the section and any information obtained under the warrant will be subject to those arrangements.

49. When exercising his/her discretion and considering necessity and proportionality, the Secretary of State must take into account *"whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means"* (s.5(2A) ISA).

50. Pursuant to s. 5(3) of the ISA GCHQ may not be granted a s.5 warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

51. By s.6 of the ISA the procedure for issuing warrants and the duration of s. 5 warrants is addressed. In particular s.6(1) provides that a warrant shall not be issued save under the hand of the Secretary of State, unless it is a species of urgent case as set out in s.6(1)(b) or (d)¹⁹.

52. In terms of duration, unless the warrant is renewed, it ceases to have effect at the end of the period of six months, beginning with the day on which it was

¹⁹ Those sub-sections provide:

(b) in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed on it, under the hand of a senior official; ...

(d) in an urgent case where the Secretary of State has expressly authorised the issue of warrants in accordance with this paragraph by specified senior officials and a statement of that fact is endorsed on the warrant, under the hand of any of the specified officials.

issued (s. 6(2)) (save where the warrant was issued urgently and not under the hand of the Secretary of State in which case it lasts for 5 working days).

53. As to renewal, under s.6(3) of the ISA, if, before the expiry of the warrant, the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, it may be renewed for a period of six months.
54. By s. 6(4) of the ISA *"The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary"*.

s.7 authorisations

55. In terms only of acts outside the British Islands, s.7 of the ISA also provides for the authorisation of such acts by the Intelligence Services including GCHQ. S.7(1) and 7(2) provide:

"(1) If, apart from this section; a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.

(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom."

56. Acts outside the British Islands include cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus (s. 7(9) ISA).²⁰
57. However, pursuant to s.7(3) of the ISA, the Secretary of State shall not give an authorisation under s. 7 of the ISA to GCHQ unless he/she is satisfied:

"(a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a function of GCHQ; and

(b) that there are satisfactory arrangements in force to secure –

(i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of ...GCHQ; and

(ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and

²⁰ In addition ss.7(10)-(14) of the ISA recognise that it may be difficult, in certain circumstances to ascertain reliably the location of property and therefore provide, *inter alia*, that where acts are done in relation to property which is eg. mistakenly believed to be outside the British Islands, but which is done before the end of the 5th working day on which the presence of the property in the British Isles first becomes known, those acts will be treated as done outside the British Islands.

(c) that there are satisfactory arrangements in force under section... 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

58. Under s. 7(4) of the ISA such an authorisation by the Secretary of State:

"(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;

(b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified."

59. Consequently the type of acts which may be covered by a s. 7 authorisation are broadly defined in the ISA and can clearly cover equipment interference outside the British Islands, where the tests in s. 7(3) of the ISA are satisfied.

60. By s. 7(5) of the ISA, an authorisation shall not be given except under the hand of the Secretary of State, or in an urgent case and where the Secretary of State has expressly authorised it to be given under the hand of a senior official.

61. In terms of duration, unless it is renewed, a s. 7 authorisation ceases to have effect at the end of the period of six months beginning on the day on which it was given (save if it was not given under the hand of the Secretary of State in which case it lasts for 5 working days) (see s. 7(6) ISA).

62. Pursuant to s. 7(7) the authorisation can be renewed for a period of six months, if the Secretary of State considers it necessary to continue to have effect for the purpose for which it was given.

63. By s. 7(8) of the ISA *"The Secretary of State shall cancel an authorisation if he is satisfied that the action authorised by it is no longer necessary"*.

64. Consequently both s. 5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that the Intelligence Services are not civilly or criminally liable for such interferences, including under the CMA.

The draft Equipment Interference Code of Practice dated February 2015 ('the EI Code')

65. The draft Equipment Interference Code of Practice was published on 6 February 2015 by the Home Office. That draft Code was issued pursuant to section 71 of RIPA and is subject to public consultation in accordance with s. 71(3) of RIPA.

66. Whilst the Code is currently in draft, as set out in the Written Ministerial Statement which accompanied its publication, it reflects the current

safeguards applied by the relevant Agencies, including GCHQ. The Agencies will continue to apply with the provisions of the draft Code throughout the consultation period and until the Code is formally brought into force. Consequently GCHQ can confirm that it complies with all aspects of the EI Code and can also confirm that it fully reflects the practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by GCHQ.

67. The EI Code provides guidance on the use by the Intelligence Services of s. 5 and s.7 of the ISA to authorise equipment interference to which those sections apply. In particular it provides guidance on the procedures that must be followed before equipment interference can take place, and on the processing, retention, destruction and disclosure of any information obtained by means of the interference.
68. To the extent that the EI Code overlaps with the guidance provided in the Covert Surveillance and Property Interference Revised Code of Practice issued in 2014 (see further below), the EI Code takes precedence, however the Intelligence Services must continue to comply with the 2014 Code in all other respects (see §1.2).
69. The EI Code also records the fact that there is a duty on the heads of the Intelligence Services to ensure that *arrangements* are in force to secure: (i) that no information is obtained by the Intelligence Services except so far as necessary for the proper discharge of their statutory functions; and (ii) that no information is disclosed except so far as is necessary for those functions (see §1.3 of the EI Code and the statutory framework under the ISA set out above).

Equipment interference to which the EI Code applies

70. The EI Code identifies specific types of equipment interference to which the code applies. At §1.6 it states:

"This code applies to (i) any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:

- a) *obtain information from the equipment in pursuit of intelligence requirements;*
- b) *obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;*
- c) *locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);*
- d) *enable and facilitate surveillance activity by means of the equipment.*

"Information" may include communications content, and communications data as defined in section 21 of the 2000 Act."

71. At §1.7 of the EI Code it summarises the effect of a s.5 warrant and states:

"The section 5 warrant process must be complied with in order properly and effectively to deal with any risk of civil or criminal liability arising from the interferences with equipment specified at sub-paragraphs (a) to (d) of paragraph 1.6 above. A section 5 warrant provides the Intelligence Services with specific legal authorisation removing criminal and civil liability arising from any such interferences."

Basis for lawful equipment interference activity

72. In addition to highlighting the statutory functions of each Intelligence Agency, the EI Code specifically draws attention to the HRA and the need to act proportionately so that equipment interference is compatible with ECHR rights. At §§1.10-1.13 the EI Code states:

"1.10 The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.

1.11 Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the Intelligence Services seek to obtain personal information about a person by means of equipment interference. Such conduct may also engage Article 1 of the First Protocol (right to peaceful enjoyment of possessions).

1.12 By section 6(1) of the 1998 Act, it is unlawful for a public authority to act in a way which is incompatible with a Convention right. Each of the Intelligence Services is a public authority for this purpose. When undertaking any activity that interferes with ECHR rights, the Intelligence Services must therefore (among other things) act proportionately. Section 5 of the 1994 Act provides a statutory framework under which equipment interference can be authorised and conducted compatibly with ECHR rights.

1.13 So far as any information obtained by means of an equipment interference warrant is concerned, the heads of each of the Intelligence Services must also ensure that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of the disclosure of that information, and that any information obtained under the warrant will be subject to those arrangements. Compliance with these arrangements will ensure that the Intelligence Services remain within the law and properly discharge their functions."

General rules on warrants

73. Chapter 2 of the EI Code contains a number of general rules on warrants issued under s. 5 of the ISA.

Necessity and proportionality

74. Within Chapter 2 the EI Code contains detailed guidance on the requirements of necessity and proportionality and how these statutory requirements are to be applied in the EI context. At §§2.6-2.8 it states:

“2.6 Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

2.7 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed interference against what is sought to be achieved;*
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.*

2.8 It is important that all those involved in undertaking equipment interference operations under the 1994 Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.”

75. Consequently the EI Code draws specific attention to the need to balance the seriousness of the intrusion against the need for the activity in operational and investigative terms, including taking into account the effect on the privacy of any other person who may be affected i.e. other than the subject of the operation. The EI Code is also very clear that it is important to consider all reasonable alternatives and to evidence what other methods were considered and why they were not implemented.

Collateral intrusion

76. The EI Code also highlights the risks of collateral intrusion involved in equipment interference and provides guidance on how any such issues should be approached, including the need to carry out an assessment of the risk of collateral intrusion. At §§2.9-2.12 it states:

“2.9 Any application for a section 5 warrant should also take into account the risk of obtaining private information about persons who are not subjects of the

equipment interference activity (collateral intrusion).

2.10 *Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the equipment interference activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.*

2.11 *All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Secretary of State fully to consider the proportionality of the proposed actions."*

77. In addition the EI Code makes clear at §2.12 that where it is proposed to conduct equipment interference activity specifically against individuals who are not intelligence targets in their own right, interference with the equipment of such individuals should not be considered as collateral intrusion but rather as "intended intrusion" and that:

"Any such equipment interference activity should be carefully considered against the necessity and proportionality criteria as described above."

Reviewing warrants

78. At §§2.13-2.15 the Code sets out certain requirements for reviewing warrants and states as follows:

"2.13 *Regular reviews of all warrants should be undertaken to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years (see Chapter 5). Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.*

2.14 *In each case, unless specified by the Secretary of State, the frequency of reviews should be determined by the member of the Intelligence Services who made the application. This should be as frequently as is considered necessary and practicable.*

2.15 *In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the Intelligence Services should consider whether it is necessary to apply for a fresh section 5 warrant."*

General best practices

79. The EI Code gives guidance on general best practice to be followed by the Intelligence Services when making applications for warrants covered by the Code. At §2.16 those requirements are:

- “• applications should avoid any repetition of information;
- information contained in applications should be limited to that required by the 1994 Act;
- where warrants are issued under urgency procedures (see Chapter 4), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and authorising officer as a priority. There is then no requirement subsequently to submit a full written application;
- where it is foreseen that other agencies will be involved in carrying out the operation, these agencies should be detailed in the application; and
- warrants should not generally be sought for activities already authorised following an application by the same or a different public authority.”

80. In addition, the EI Code indicates that it is considered good practice that within each of the Intelligence Services, a designated senior official should be responsible for:

- “• the integrity of the process in place within the Intelligence Service to authorise equipment interference;
- compliance with the 1994 Act and this code;
- engagement with the Intelligence Services Commissioner when he conducts his inspections; and
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the Commissioner.” (see §2.17)

Legally privileged and confidential information

81. Chapter 3 of the Code contains detailed provisions on legally privileged and confidential information which it is intended to obtain or which may have been obtained through equipment interference. In terms of confidential information the Code provides, *inter alia*, at §§3.24-3.27:

- “3.24 Where the intention is to acquire confidential information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to adopting special handling arrangements within the relevant Intelligence Service.
- 3.25 Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so in accordance with the statutory functions of each of the Intelligence Services or where otherwise required by law. It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, it must be reviewed at reasonable intervals to confirm that the justification for its retention is still valid
- 3.26 Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from a legal adviser within the relevant Intelligence Service before any further dissemination of

the material takes place.

- 3.27 *Any case where confidential information is retained should be reported to the Intelligence Services Commissioner during the Commissioner's next inspection and any material which has been retained should be made available to the Commissioner on request."*

Procedures for authorising equipment interference under s. 5

82. Chapter 4 of the EI Code sets out the general procedures to be followed for authorising equipment interference activity under s. 5 of the ISA. In that Chapter, §§4.1-4.4 outline the statutory scheme under the ISA. At §4.5 of the code, attention is drawn to the need to consider whether the equipment interference operation might also enable or facilitate a separate covert surveillance operation, in which case a directed or intrusive surveillance authorisation might need to be obtained under Part 2 of RIPA (as addressed in the Covert Surveillance and Property Interference Code).

83. In terms of applications for a s. 5 warrant, the EI Code contains a checklist of the information which each issue or renewal application should contain. At §4.6 it states:

"An application for the issue or renewal of a section 5 warrant is made to the Secretary of State. Each application should contain the following information:

- the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference;*
- sufficient information to identify the equipment which will be affected by the interference;*
- the nature and extent of the proposed interference, including any interference with information derived from or related to the equipment;*
- what the operation is expected to deliver and why it could not be obtained by other less intrusive means;*
- details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected.*
- whether confidential or legally privileged material may be obtained. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege or confidential personal information, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;*
- details of any offence suspected or committed where relevant;*
- how the authorisation criteria (as set out at paragraph 4.7 below) are met;*
- what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);*
- where an application is urgent, the supporting justification;*
- any action which may be necessary to install, modify or remove software on the equipment;*
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results."*

84. At §4.7-§4.9 of the EI Code the statutory tests for the issuing of a s. 5 warrant

are highlighted, together with the statutory requirements for any urgent authorisation of a s. 5 warrant.

Renewals and cancellations of warrants

85. At §§4.10-4.11 and §§4.12-4.13 of the EI Code the provisions of the ISA addressing the renewals and cancellations of warrants are summarised.

Keeping of records

86. In Chapter 5 of the EI Code provision is made for centrally retrievable records of warrants to be kept for at least three years. At §5.1 it states:

"The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:

- *the date when a warrant is given;*
- *the details of what equipment interference has occurred;*
- *the result of periodic reviews of the warrants;*
- *the date of every renewal; and*
- *the date when any instruction was given by the Secretary of State to cease the equipment interference."*

Handling of information and safeguards

87. Chapter 6 of the EI Code provides important guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant and makes clear that this information may include communications content and communications data as defined in section 21 of RIPA (§6.1).

88. At §6.2 the EI Code states:

"The Intelligence Services must ensure that their actions when handling information obtained by means of equipment interference comply with the legal framework set out in the 1989 and 1994 Acts (including the arrangements in force under these Acts), the Data Protection Act 1998 and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with this legal framework will ensure that the handling of information obtained by equipment interference continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards against abuse."

89. At §§6.6-6.11 of the EI Code key safeguards are set out in the EI Code in terms of the dissemination, copying, storage and destruction of any information obtained as a result of equipment interference. In particular it is stated:

"Dissemination of information

- 6.6 *The number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary for the proper discharge of the Intelligence Services'*

functions or for the additional limited purposes described in paragraph 6.5. This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: information obtained by equipment interference must not be disclosed to any person unless that person's duties are such that he needs to know about the information to carry out those duties. In the same way only so much of the information may be disclosed as the recipient needs; for example if a summary of the information will suffice, no more than that should be disclosed.

- 6.7 *The obligations apply not just to the Intelligence Service that obtained the information, but also to anyone to whom the information is subsequently disclosed. In some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further. In others, explicit safeguards may be applied to secondary recipients.*

Copying

- 6.8 *Information obtained by equipment interference may only be copied to the extent necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. Copies include not only direct copies of the whole of the information, but also extracts and summaries which identify themselves as the product of an equipment interference operation. The restrictions must be implemented by recording the making, distribution and destruction of any such copies, extracts and summaries that identify themselves as the product of an equipment interference operation.*

Storage

- 6.9 *Information obtained by equipment interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store such information securely applies to all those who are responsible for the handling of the information.*

Destruction

- 6.10 *Communications content, communications data and other information obtained by equipment interference, and all copies, extracts and summaries thereof, must be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes set out in paragraph 6.5. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid."*

Personnel security

6.11 *In accordance with the need-to-know principle, each of the Intelligence Services must ensure that information obtained by equipment interference is only disclosed to persons as necessary for the proper performance of the Intelligence Services' statutory functions. Persons viewing such product will usually require the relevant level of security clearance. Where it is necessary for an officer to disclose information outside the service, it is that officer's responsibility to ensure that the recipient has the necessary level of clearance.*" (emphasis added)

90. At §§6.4-6.5 the importance of these safeguards is emphasised, together with the need to ensure that each of the Intelligence Services has internal arrangements in force for securing that the safeguards are satisfied, which arrangements should be made available to the Intelligence Services Commissioner. In particular it is stated:

"6.4 Paragraphs 6.6 to 6.11 provide guidance as to the safeguards which must be applied by the Intelligence Services to the processing, retention, disclosure and destruction of all information obtained by equipment interference. Each of the Intelligence Services must ensure that there are internal arrangements in force, approved by the Secretary of State, for securing that these requirements are satisfied in relation to all information obtained by equipment interference.

6.5 These arrangements should be made available to the Intelligence Services Commissioner. The arrangements must ensure that the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act. Breaches of these handling arrangements must be reported to the Intelligence Services Commissioner as agreed with him."

Application of the code to equipment interference pursuant to section 7 of the 1994 Act

91. In Chapter 7 of the EI Code it is made clear that "GCHQ must as a matter of policy apply the provisions of this code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands" (§7.1).

92. Consequently, save as expressly specified in Chapter 7 of the EI Code, all of the provisions of the EI Code, including the important safeguards regarding the processing, retention, disclosure deletion and destruction of any information obtained via equipment interference, apply equally to equipment interference authorised pursuant to s. 7 of the ISA. That is made expressly clear in §7.2 which states:

"GCHQ and SIS must apply all the same procedures and safeguards when conducting equipment interference authorised pursuant to section 7 as they do in relation to equipment interference authorised under section 5."

93. In addition, Chapter 7 of the EI Code provides specific additional guidance for s. 7 equipment interference authorisations under the ISA.

94. In terms of the general basis for lawful activity under s. 7 of the ISA, the EI Code states at §§7.3-7.6:

“7.3 *An authorisation under section 7 of the 1994 Act may be sought wherever members of SIS or GCHQ, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located outside the British Islands that would otherwise be unlawful. This includes cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus*^[21].”

7.4 *If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a ‘grace period’ of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period).*

7.5 *An application for a section 7 authorisation should usually be made by a member of SIS or GCHQ for the taking of action in relation to that service. Responsibility for issuing authorisations under section 7 rests with the Secretary of State.*

7.6 *An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations. Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference must be sought from a designated senior official (see paragraphs 7.11 to 7.14).“*

95. At §§7.7-7.8 and §§7.9-7.10 the EI Code sets out the statutory tests for s. 7 authorisations, together with the provisions of the statutory scheme dealing with urgent authorisations. At §7.7 the EI Code makes clear that:

“Each application should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 equipment interference warrant.”

²¹ However this is “without prejudice as to arguments regarding the applicability of the ECHR” as made clear in footnote 17 of the EI Code.

96. Guidance on the types of authorisations under s.7 of the EI Code is also provided at §§7.11-7.14. In particular this provides guidance on any s. 7 authorisations which relate to a broad class of operations. At §§7.11-7.12 it states:

"7.11 An authorisation under section 7 may relate to a broad class of operations. Authorisations of this nature are referred to specifically in section 7(4)(a) of the 1994 Act which provides that the Secretary of State may give an authorisation which inter alia relates to "acts of a description specified in the authorisation". The legal threshold for giving such an authorisation is the same as for a specific authorisation.

7.12 Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference must be sought from a designated senior official. In any case where the equipment interference may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer. Where knowledge of matters subject to legal privilege may be acquired, the Annex A approving officer must apply the tests set out at paragraph 3.4 to 3.7 (and "Secretary of State" should be read as "Annex A approving officer" for these purposes).

97. For GCHQ an 'Annex A approving officer' means a Director of GCHQ (see Annex A on page 30).

98. In addition §§7.13-7.14 provide guidance on all internal applications for approval, including the need to ensure that such approvals are proportionate and are subject to periodic review at least every 6 months, or more frequently depending on the sensitivity of the operation. Those paragraphs state:

"7.13 The application for approval must set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer must be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer must consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations.

7.14 All internal approvals must be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case."

99. As to renewals and cancellations of s. 7 authorisations, the statutory requirements are set out at §§7.15-7.17.

- 99A. For the avoidance of doubt, and in the light of the clarification requested at

paragraph 47A(b) of Privacy's Amended Grounds, it is the Respondents' position that it is lawful for a s.7 authorisation to relate to a broad class of operations, without a specific and individual "warrant" being made in respect of each individual operation conducted pursuant to that authorisation. As set out above, the EI Code provides for a process of internal approval by a designated senior official to conduct operations under that authorisation.

Internal arrangements

99B. GCHQ also has internal arrangements in relation to s.5 warrants and s.7 authorisations. These are set out below, with gisted passages underlined.²²

The Compliance Guide

99C. The Compliance Guide is a document which is made available electronically to all GCHQ staff. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity must be:

- a) Authorised (generally through a warrant or equivalent legal authorisation);
- b) Necessary for one of GCHQ's operational purposes; and
- c) Proportionate.

99D. These principles, and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.

99E. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

"A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ

²² The internal arrangements are set out at §§99C to 99Z5. They are added by way of amendment but are not underlined in order to make it clear which passages are gisted.

official of appropriate seniority if a Secretary of State has expressly authorised its use."

Section 5 Guidance

99F. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants ("the Section 5 Guidance"). The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target's privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

99G. The Section 5 Guidance makes clear the nature of the activity which is authorised by a s.5 warrant:

"ISA Section 5 guidance

ISA warrants

Warrants issued under the Intelligence Services Act (ISA) authorise interference with property (eg equipment such as computers, servers, routers, laptops, mobile phones, software, intellectual property etc) or wireless telegraphy."

99H. The geographical, functional and temporal limits of a s.5 warrant are also set out:

"A section 5 warrant authorises interference with property or wireless telegraphy in the British Islands²³...It may only be issued on grounds of National Security or the Economic Well-Being of the UK. A section 5 warrant is signed by a Secretary of State and is valid for 6 months from the date of signature, at which point the warrant should be renewed or cancelled."

99I. The guidance mirrors the requirements of s.5(2)(a) and (b) of the ISA. First, it makes clear that the proposed CNE action must be **necessary**:

"Part I. - to be completed by the relevant GCHQ team

The intelligence case should be fit for purpose for signing by a Secretary of State, avoiding unnecessary jargon and technical terminology. The case should include:

- *the intelligence background;*

²³ Both instances of underlining in this quotation are in the original.

- *the priority of the target within the priorities framework as endorsed by JIC²⁴ and NSC²⁵;*
- *an explanation of why the proposed operation is necessary;*
- *a description of any other agency involvement in working the target;*
- *the intelligence outcome(s) the proposed operation is expected to produce.”*

99J. The requirement that the proposed CNE action be **proportionate** is also made clear:

“As CNE techniques are by nature intrusive, an explanation of how proportionality will be maintained should be given. Key points to consider include:

- *the expected degree of invasion of a target’s privacy and whether any personal or private information will be obtained;*
- *the likelihood of collateral intrusion, ie invading the privacy of those who are not targets of the operation, eg family members;*
- *whether the level of intrusion is proportionate to the expected intelligence benefit;*
- *a description of the measures to be taken to ensure proportionality.”*

99K. The Section 5 Guidance stipulates that each request for a warrant, or warrant renewal, must have a sponsor of an appropriately senior level:

“Requesting a new Section 5

Requests for new warrants and renewals must be sponsored by an appropriately senior official, who must be satisfied that the proposed operation is justified, proportionate and necessary.”

99L. The Section 5 Guidance requires that, once completed, the warrant request must be returned to its “sponsor” for consideration of whether it passes the test set out in s.5(2)(a) and (b) of the ISA, before being signed and sent to the relevant personnel:

“The form is then returned to the sponsor to consider whether, in light of the CNE input, they can recommend to the Secretary of State that the operation is justified, proportionate and necessary, and that they are aware of the risk. If so, they should sign and date the form and send it to the relevant personnel.”

99M. The Section 5 Guidance also explains that the process is completed by the preparation of a formal submission and a warrant instrument. These are reviewed by GCHQ Legal Advisers and the sponsor, then sent for signature to the relevant Department, which will follow its own internal procedures before the documents are passed to the Secretary of State for consideration. Once the warrant has been signed, relevant personnel will be informed that the operation can go ahead.

99N. A designated form must be filled out when a section 5 warrant is sought. The specified information reflects the requirements of the guidance on section 5 warrants, and includes the following:

²⁴ Joint Intelligence Committee.

²⁵ National Security Council.

a) Under "Intelligence Case"

"why is CNE necessary and why can the expected intelligence not be gained by other less intrusive means?"

"what intelligence the operation is expected to deliver"

b) Under "Degree of intrusion, including collateral intrusion"

"how far will the operation intrude on the privacy of the target? Is the operation likely to obtain personal or private information?"

to what extent will the operation affect those not of operational interest (eg could the individual's computer be used by family members, friends or colleagues who are not targets of the operation)?

how will the intelligence gained justify the expected level of intrusion?

what measures will be put in place to ensure proportionality is maintained."

(c) Under "Recipients of Product":

"where within GCHQ is the product of the CNE operation to be sent?"

(d) Finally, the Request must be authorised by the appropriately senior GCHQ official, who must, inter alia, certify that "The proposed CNE operation is justified, proportionate and necessary".

Renewals of s.5 warrants

990. The Section 5 Guidance also details the procedure for renewals of section 5 warrants. This requires specific attention to be paid, *inter alia*, to whether the operation is still justified, necessary and proportionate at the time of the renewal:

"Section 5 renewal process

A reasonable period before a warrant is due to expire, the relevant personnel will request a case for renewal from the relevant personnel, copying the sponsor and include a copy of the previous submission. The analyst should confirm with the sponsor that renewal is required, and if so, provide the relevant personnel with a business case by the specified deadline. This should include:

- an update of the intelligence background, ensuring it accurately reflects the current context of the warrant;*
- details of any developments and intelligence gained since the warrant was issued/last renewed - this **must** address any expectations highlighted in the previous submissions;*
- a review of the level of intrusion, based on the evidence of the activity authorised by the warrant;*
- a review and, if necessary, update of the political aspects of the risk assessment;*

²⁶ Underlining in the original.

The relevant team should provide the following information:

- any updates on technical progress made since the warrant was last renewed
- an updated operational plan – again, this **must** address specific actions or plans laid out in the previous submission
- any updates to the risk assessment.

Again, the relevant personnel may need to work with the originator and the relevant team to strengthen the renewal case, and will also consult the Legal Advisers before providing a copy to the sponsor for final review. When the sponsor is content that the submission is accurate and demonstrates that the operation is still justified, necessary and proportionate, the relevant personnel will submit the renewal application to the relevant Department for signature.”

Cancellation of s.5 warrants

99P. The Section 5 Guidance also addresses cancellation of warrants, making clear that as soon as warrants are no longer required they should be cancelled:

“If a warrant is no longer required, it should be cancelled. If not renewed or cancelled, the warrant will expire on the date specified and the activity will no longer be authorised.

It is good practice to cancel warrants as soon as the requirement for the operation has ceased.

Section 5 cancellation process

When a warrant is no longer required, the analyst should send the relevant personnel a short explanation of the reason for the cancellation. When the team conducting the operation confirms that the operation is fully drawn down, the relevant personnel will draft a letter based on this feedback and submit it, with a cancellation instrument, to the issuing Department for signature (usually by a senior official rather than the Secretary of State).”

Section 7 Guidance

99Q. GCHQ’s guidance which governs applying for, renewing and cancelling section 7 authorisations/internal approvals is set out both in the Compliance Guide (in the section dealing with authorisations) and in separate internal guidance (“the Section 7 Guidance”). The process set out in the Section 7 Guidance has been subject to the scrutiny and advice of the Intelligence Services Commissioner who has confirmed that he is content with the process.²⁷

²⁷ In addition to the Intelligence Services Commissioner’s suggestions in his June 2013 inspection, and his approval of GCHQ’s consequent changes in his December 2013 inspection, during a visit in December 2014 GCHQ presented to and discussed with the Intelligence Services Commissioner, the “end to end” process regarding CNE operations using two operational case-studies. The class-authorisation, internal approvals and additions authorisations were considered. The Commissioner was then shown how CNE operators conduct the operations with a live demonstration of an operation. There was also a focus on the relevant forms (which were discussed in some detail). The Commissioner indicated that he was content with the format and the level of detail in the forms.

- 99R. The Section 7 Guidance requires any CNE activities overseas to be carried out pursuant to a s.7 authorisation in order for such activities to be lawful under domestic law. Authorisations may either be specific to a particular operation or to a broad class of operation:

"ISA Section 7 guidance

ISA authorisations

An ISA s7 authorisation given by the Secretary of State is the legal instrument that removes criminal liability in the UK for GCHQ actions overseas which might otherwise be an offence in UK law. Such an authorisation is also capable of removing any civil liability in the UK that might arise as a result of GCHQ's actions overseas. GCHQ primarily uses s7 authorisations for CNE operations. An ISA s7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations..."

- 99S. The Section 7 Guidance sets out the 'class authorisations' signed by the Secretary of State under section 7 of the ISA which are used by GCHQ for the majority of its active internet-related operations. In respect of the authorisations relevant to CNE the Section 7 Guidance states that it:

"permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant). The interference includes CNE operations."

- 99T. The Section 7 Guidance also stipulates that such authorisations need to be renewed every six months, and assert the vital importance of providing information to the Secretary of State to justify any renewal:

"Class authorisations are signed by the Foreign Secretary and need to be renewed every six months. Relevant personnel in GCHQ are responsible for overseeing the renewal process. Prior to expiry of the authorisations, they will ask analysts to briefly (re)justify the necessity and proportionality of continuing to rely on all extent section 7 internal approvals for which they are the lead, as well as asking for feedback on the outcomes of operations conducted. Providing feedback to the Foreign Secretary on the value of operations conducted under the class authorisations is crucial in justifying their renewal."

- 99U. The requirement, in addition to a section 7 class authorisation, for a section 7 approval for a specific operation, and the procedure for obtaining such an approval, is set out both in the section of the Compliance Guide on CNE, and also in the Section 7 Guidance. The latter emphasises, *inter alia*, the importance of considering and setting out, in a request for a section 7 approval, why an operation against a target is necessary and proportionate, and the requirement that a copy of the signed approval be sent to the FCO:

"ISA section 7 internal approvals

A condition of section 7 authorisations is that GCHQ operates an internal section 7 approval process to record its reliance on these authorisations. Before tasking the operational team to conduct CNE operations, analysts are required to complete a request form including a detailed business case described the necessity and proportionality of conducting operations against the targets. The request also sets out the likely political risk. The request must be endorsed by a senior member of the operational team before it is passed to an appropriately senior official for approval...A copy of the signed final version of the approval is sent to FCO for information."

- 99V. The Section 7 Guidance explains the importance of this process, including the provision of signed approvals to the FCO, for ensuring that operations are necessary, justified and proportionate is again stressed:

"This process provides the necessary reassurance to FCO that operations carried out under the class authorisations are necessary, justified and proportionate."

- 99W. Necessity (including why means other than a CNE operation could not be used) and proportionality (particularly with regard to the privacy of a target or any third party) are addressed in more detail under "Section B - business case/necessity/proportionality":

"The business case should...include:

- the intelligence background;*
- the priority in the priorities framework;*
- an explanation of why the operations against the target set are necessary;*
- the intelligence outcome(s) the proposed CNE activities are expected to produce."*

You should also consider the level of intrusion the proposed operations will involve and how proportionality will be maintained. Key points to consider include:

- the expected degree of intrusion into a target's privacy and whether any personal or private information will be obtained;*
- the likelihood of collateral intrusion, i.e. invading the privacy of those who are not targets, such as family members;*
- whether the level of intrusion is proportionate to the expected intelligence benefit;*
- any measures to be taken to ensure proportionality."*

- 99X. The Section 7 Guidance makes clear, under "Completing the process" that the internal approval will then be provided to an appropriately senior GCHQ official for signature and for, *inter alia*, the setting of a review period for the internal approval:

"Based on all the information provided, relevant personnel will ensure that the section 7 internal approval is suitable for referral to an appropriately senior GCHQ official for signature. That official will review all the matters relevant to the application to satisfy himself that the proposed activity is justified, necessary and proportionate, including validating the assessment of political risk. He will also set the review period for the internal approval, which will be shorter for particularly sensitive operations."

99Y. The standard form used for seeking section 7 approvals reflects both the Section 7 Guidance and the statutory criteria. In particular it sets out the following:

- a) *“Business case, including*
 - *Intelligence background (to include brief details of what has been achieved from other accesses).*
 - *What you expect to get from using CNE techniques against this target set & how the intelligence gained will justify the expected level of intrusion.*
 - *Any timing factors or special sensitivities.**...”*
- b) *“Necessity, including*
 - *The necessity of conducting CNE operations against this target set (an explanation of why the use of CNE techniques is necessary).”*
- c) *“Proportionality and consideration of intrusion into privacy, including*
 - *The proportionality of conducting CNE operations against this target set (CNE operations are intrusive by nature, and are likely to obtain information which is personal and private). Confirm that you have assessed that the level of intrusion into privacy, including collateral intrusion, is justified and proportionate. Outline measures to be put in place to ensure proportionality is maintained.”*

The term “privacy” is defined “in the broadest sense to mean a state in which one is not observed or disturbed by others”.

99Z. The appropriately senior GCHQ official who must support any request for a section 7 approval has to certify, *inter alia*, that:

“Operations conducted under this approval are justified, proportionate and necessary.”

99ZA. The relevant form also makes clear that the request for an approval should be sent to the relevant personnel at request stage, review stage and cancellation stage. Where an addition to an approval is sought the relevant personnel must also be consulted.²⁸ As a matter of practice, and as required by the Section 7 Guidance, final versions of s.7 approvals are sent to the Foreign and Commonwealth Office. A monthly summary report which summarises new s.7 approvals, reviews of s.7 approvals and cancellations, and also attaches copies of new approvals, is also sent to the relevant senior official at the FCO.

99ZB. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an “addition” to an existing approval is required.

99ZC. The “additions form” requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

²⁸ A reference to “relevant personnel” is to staff who are responsible for securing legal/policy approvals, checking the relevant risk assessments and maintaining compliance records.

Review of s.7 internal approvals

- 99ZD. Approvals must be reviewed, and upon each review consideration is required to be given to whether the operation is still necessary and proportionate, specifically having regard to issues of intrusion and privacy. The process of reviewing s.7 approvals is summarised in the Section 7 Guidance as follows:

“Reviewing section 7 internal approvals

In addition to the reviews that are carried out in support of the renewal of the class authorisations when analysts are required to briefly (re)justify the necessity and proportionality of continuing to rely on all extant internal approvals for which they are the lead, there is a rolling programme of fully revalidating all extant section 7 internal approvals. This revalidation mirrors the process for obtaining a new internal approval: an updated business case (covering justification, necessity, proportionality and intrusion into privacy) is provided by the lead analyst; the operational team confirm that they are still operating within the risk thresholds set when the internal approval was signed; the endorser confirms that the assessment of the likely political risk is still correct; then continued operations may be approved and a new review date set if no significant changes have been made (or the review of the approval is passed to a GCHQ official of appropriate seniority.”

- 99ZE. The review and revalidation is held at intervals determined by the designated GCHQ senior official who originally signed the section 7 approval. These are more frequent for particularly sensitive operations. The Section 7 Guidance also sets out a procedure for recording the history of a section 7 approval from the original submission through to any review or cancellation:

“New review history and cancellation forms will be appended at each review point. The intention is to leave the original submission intact, so that there is an audit trail of what was originally submitted/approved. If there are any updates to be made, these will be included in the review history so that there is an ongoing record at each review of what was decided and why.”

- 99ZF. Thus the approval process, including any review, is recorded so that the history of and basis (including necessity and proportionality) for any approval, review or cancellation, is available for audit.

Cancellation of s.7 internal approvals

- 99ZG. The Section 7 Guidance also stipulates the need to cancel internal approvals as soon as an operation is no longer needed:

“Cancelling a section 7 internal approval

To show due diligence and as a condition of relying on the class authorisations, section 7 internal approvals should be cancelled when an operation is no longer needed. To help ensure that this happens, the relevant personnel will ask whether section 7 internal approvals are still needed as part of the class authorisation renewals process, and if so will seek a brief rejustification of the continuing necessity and

proportionality. The number of approvals signed or cancelled is provided to the Foreign Secretary with the case for renewal.

It is important to cancel an internal approval as soon as it is no longer required.

When a section 7 internal approval is no longer required, the analyst should ask the operational team point of contact to cease operations and remove all tasking. The relevant personnel will not formally cancel the approval until the operational team confirms that the operation is fully drawn down."

99ZH. The Section 7 Guidance therefore contains safeguards against section 7 approvals remaining in place where they are no longer necessary and/or proportionate.

Obtaining data

99ZI. There are further safeguards in place to ensure that decisions by CNE operators to obtain data from implanted devices are lawful. In particular:

- a) In addition to a formal process of training and examination which all CNE Operators have to undergo, all CNE operators must every two years also undertake advanced legalities training which is specific to active operations such as CNE (in addition to the basic legalities training which all staff are required to complete).
- b) CNE operators can obtain legal advice at any time.
- c) In addition, any data obtained in an operation will be available to the relevant intelligence analysts for that project, who in turn will be aware of the legal authorisation for the project, and will also have completed legalities training. The CNE section of the Compliance Guide provides guidance for intelligence for intelligence analysts requesting a particular document to be retrieved.

99ZJ. Thus, the obtaining of data is subject to the same requirements of necessity and proportionality as the initial process of obtaining an authorisation/warrant/approval.

Storage of and access to data

99ZK. GCHQ also has policies for storage of and access to data obtained by CNE.

99ZL. The section of the Compliance Guide concerning "Review and Retention" states that GCHQ treats "all operational data" (i.e. including that obtained by CNE) as if it were obtained under RIPA. It sets out GCHQ's arrangements for minimising retention of data in accordance with RIPA safeguards. This is achieved by setting default maximum limits for storage of operational data.

99ZM. In addition GCHQ has a separate policy specifically concerning data storage and access. It defines different categories of data, and importantly ascribes

specific periods for which different categories of data may be kept, as well as explaining how different categories of CNE data relate to the categories of operational data set out in the Compliance Guide.

- 99ZN. Where CNE analysts identify material as being of use for longer periods than the stipulated limits, it can be retained for longer, subject to justification according to specific criteria.
- 99ZO. Access to data is also subject to strict safeguards, which are set out in the Compliance Guide. CNE content may be accessed by intelligence analysts, but they must first demonstrate that such access is necessary and proportionate by completing a Human Rights Act ("HRA") justification. HRA justifications are recorded and made available for audit. CNE technical data relating to the conduct of CNE operations may only be accessed by a team of trained operators responsible for planning and running such operations.
- 99ZP. GCHQ's policy on storage of and access to data also requires GCHQ analysts who are not in the CNE operational unit to justify access to CNE data on ECHR grounds (particularly necessity and proportionality). The justification must be recorded and available for audit.

Handling/disclosure/sharing of data obtained by CNE operations

- 99ZQ. Pursuant to GCHQ's Compliance Guide, the position is that all operational material is handled, disclosed and shared as though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.
- 99ZR. The general rules, as set out in the Compliance Guide and the Intelligence Sharing and Release Policy which apply to the handling of operational material include, *inter alia*, a requirement for mandatory training on operational legalities and detailed rules on the disclosure of such material outside GCHQ and the need to ensure that all reports are disseminated only to those who need to see them.
- a) Operational data cannot be disclosed outside of GCHQ other than in the form of an intelligence report.
- b) Insofar as operational data comprises or contains confidential information (e.g. journalistic material) then any analysis or reporting of such data must comply with the "Communications Containing Confidential Information" section of the Compliance Guide. This requires GCHQ to have greater regard to privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved (e.g. legally privileged material, confidential personal information, confidential journalistic information, communications with UK legislators). GCHQ must accordingly demonstrate to a higher level than normal that retention and dissemination of such information is necessary and proportionate.

Training

- 99ZS. In addition to the training referred to at paragraphs 99ZI(a) and 99ZR above, GCHQ does provide some training for analysts on particular CNE activities, which reiterates the substance of the Section 7 Guidance. GCHQ is currently in the process of revising the training referred to at paragraph 99ZI(c) to incorporate more detail on CNE.

Oversight by the Intelligence Services Commissioner

100. In §§8.1-8.2 of the EI Code the important role of the Intelligence Services Commissioner in the use of the powers under the ISA is emphasised. In particular §8.2 states:

"It is the duty of any member of the Intelligence Services who uses these powers to comply with any request made by the Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions. Such persons must also report any action that is believed to be contrary to the provisions of the 1994 Act to the Commissioner."

The Covert Surveillance and Property Interference Code ("the Property Code")

101. The Covert Surveillance and Property Interference Code ("the Property Code") provides guidance on entry on and interference with property by public authorities under s. 5 of the ISA (see the Code at §1.2) and applied to activity including equipment interference. That Code was also issued pursuant to s. 71 of RIPA which stipulates that the Secretary of State shall issue one or more codes of practice in relation to the powers and duties in, *inter alia*, s.5 of the 1994 Act. The Property Code was first issued in 2002 and further versions of the Code were published in 2010 and on 10 December 2014 (in terms of property interference there is no material difference between the 2010 and the 2014 versions of the Code).
102. As set out above, to the extent that there is an overlap between the EI Code and the Property Code, the EI Code takes precedence in terms of equipment interference under s. 5 of the ISA. In those circumstances the Respondents have set out below only a brief overview of the key provisions of the Property Code.
- (a) Chapter 3 of the Code contains general rules on authorisations, *inter alia*, under s. 5 of the ISA and in particular guidance is given as to the requirement of proportionality and the factors to be taking into account when making a proportionality assessment.
 - (b) The question of collateral intrusion is also directly addressed in §§3.8ff of the Code.
 - (c) As to the procedures to be followed for reviewing authorisations, the Code provides for regular reviews of all property interference authorisations (see §§3.23-3.25).
 - (d) The Code also highlights best working practices which are to be followed by all public authorities with regard to all activities covered

- by the Code (see §§3.28-3.29).
- (e) Chapter 4 of the Code contains special provisions on legally privileged and confidential information.
 - (f) Chapter 7 of the Code contains authorisation procedures for property interference. This specifically addresses authorisations for property interferences by the Intelligence Services at §§7.36-7.38.
 - (g) Chapter 8 of the Code provides that certain records shall be kept of property interferences which are authorised which are to be centrally retrievable for three years (see in particular §8.3).
 - (h) In Chapter 9 of the Code guidance is given as to the handling of material obtained through property interference. §9.3 of the Code addresses the retention and destruction of material and states as follows:

"9.3 Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of ... property interference..."
 - (i) In addition the Code states at §9.7 that, in relation to the Intelligence Services:

"9.7 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the ... 1994 Act."
 - (j) Finally Chapter 10 of the Code highlights the oversight which is provided by the Intelligence Services Commissioner on the use of the powers under the ISA. At §10.2 it states:

"The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within ... the 1994 Act by ... GCHQ."

The HRA

103. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:
- "(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*
- (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."*
104. Art. 10 of the ECHR, which is similarly a Convention right (and which is similarly set out in Sch. 1 to the HRA), provides:
- "(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema"*

enterprises.

(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

105. By s. 6(1):

"It is unlawful for a public authority to act in a way which is incompatible with a Convention right."

106. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, GCHQ must (among other things) act proportionately and in accordance with law. In terms of equipment interference activity, the HRA applies at every stage of the process i.e. from authorisation, through to the obtaining, retention, handling and any disclosure/dissemination of such material.

107. S. 7(1) of the HRA provides in relevant part:

"A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may –

(a) bring proceedings against the authority under this Act in the appropriate court or tribunal"

The DPA

108. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data (as defined in s. 1(1) of the DPA) that it holds. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

109. Consequently as a data controller, GCHQ is in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "is required for the purpose of safeguarding national security". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services (including GCHQ) are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do not exempt the Intelligence Services (including GCHQ) from their obligation to comply with the fifth and seventh data protection principles, which provide:

"5. Personal data processed²⁹ for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. ...

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."³⁰

110. Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged:
- (a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and
 - (b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

111. A member of the Intelligence Services commits an offence if *"without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services"*: s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of GCHQ that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).
112. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

Oversight mechanisms

113. There are three principal oversight mechanisms in respect of the equipment interference regime:
- (a) The Intelligence Services Commissioner

²⁹ The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

³⁰ The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

- (b) The ISC; and
- (c) The Tribunal.

The Intelligence Services Commissioner

114. As highlighted in the relevant Code, the Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within the ISA by the Intelligence Services including GCHQ.
115. The Prime Minister is under a duty to appoint a Commissioner (see s. 59(1) of RIPA). By s. 59(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner is currently Sir Mark Waller.
116. Under s. 59(7) of RIPA, the Commissioner must be provided with such staff as are sufficient to ensure that he can properly carry out his functions. Those functions include those set out in s. 59(2), which provides in relevant part:
- "...the [Commissioner] shall keep under review, so far as they are not required to be kept under review by the Interception of Communications Commissioner-*
- (a) the exercise by the Secretary of State of his powers under sections 5 to 7 of... the Intelligence Services Act 1994..."*
117. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 60(1) of RIPA.
118. In practice, the Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Representative samples of warrantry paperwork are scrutinised, including the paperwork for s. 5 and/or s.7 ISA warrants/authorisations. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Commissioner also meets with the relevant Secretaries of State.
119. S. 60 of RIPA imposes important reporting duties on the Commissioner. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.)
120. The Commissioner is by s. 60(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 60(3)). Pursuant to s. 60(4), a copy of each annual report (redacted, where necessary under s.60(5)), must be laid before each House of Parliament. In this way, the Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed

openly.

121. S. 58(5) grants the Commissioner power to make, at any time, any such other report to the Prime Minister on any other matter relating to the carrying out of his functions as he thinks fit.
122. In addition, the Commissioner is required by s. 59(3) to give the Tribunal:

"...such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-
(a) in connection with the investigation of any matter by the Tribunal; or
(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter."
123. The Tribunal is also under a duty to ensure that the Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).
124. The Commissioner's oversight functions are supported by the record keeping obligations that are imposed as part of the equipment interference regime, see §8.3 of the Code.
125. It is to be noted that in the *Liberty/Privacy* judgment the Tribunal placed considerable emphasis on the important oversight which is provided by the Interception Commissioner (see in particular §§24, 44, 91, 92 121 and 139 of the judgment) and a similarly important role is provided by the Intelligence Services Commissioner in the present context.

The ISC

126. GCHQ is responsible to the Foreign Secretary,³¹ who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.
127. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 ("the JSA").
128. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.
129. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a

³¹ The Director of GCHQ must make an annual report on the work of GCHQ to the Prime Minister and the Secretary of State (see s. 4(4) of the ISA).

member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

- ~~130. The current chair is Sir Malcolm Rifkind MP. He is a former Secretary of State for Defence and a former Secretary of State for Foreign and Commonwealth Affairs.~~
131. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.
132. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.
133. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.
134. It is to be noted that in the *Liberty/Privacy* judgment, the Tribunal placed considerable emphasis on the important oversight which is provided by the ISC (see in particular §44 and §121 of the judgment); the Tribunal describing the ISC as "*robustly independent*" at §121.

The Tribunal

135. The Tribunal was established by s. 65(1) of RIPA. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).
136. The Tribunal's jurisdiction is broad. As regards the Equipment Interference regime, the following aspects of the Tribunal's jurisdiction are of particular relevance:
- (a) The Tribunal has exclusive jurisdiction to consider claims under s.

7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

(b) The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) of RIPA).

137. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).
138. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained, interfered with or disclosed information emanating from interferences with property/equipment in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged obtaining, interference with or disclosure of information.
139. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.³² As a result, the Tribunal is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.
140. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §138~~138~~ above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.
141. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.
142. Subject to any provision in its rules, the Tribunal may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

³² The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish e.g. that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

ISSUE OF PURE LAW SUITABLE FOR DETERMINATION AT A LEGAL ISSUES HEARING

143. It is submitted that the following issue of pure law can be identified from the Grounds advanced by the Claimants:

Issue: Does the Equipment Interference Regime satisfy the “in accordance with the law” requirement in Art. 8(2)?

144. The remaining grounds of claim do not give rise to pure issues of law which are suitable for determination at a Legal Issues Hearing. Rather, these grounds of claim turn on factual assertions that are neither confirmed nor denied, and which are relevant to the determination of the “proportionality” issues raised. It follows that they must - as necessary - be investigated and considered by the Tribunal in closed session in the light of such relevant closed evidence, if any, as is filed by the Respondents. The Respondents invite the Tribunal to investigate these grounds of claim in closed session after holding a Legal Issues Hearing.
145. As set out earlier in this Response, Article 10 adds nothing to the analysis under Article 8 ECHR - see §147 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5 and see also §12 and §149 of the *Liberty/Privacy* judgment and therefore this has not been addressed separately below. In addition the A1P1 complaint on the part of the Greenet Claimants (1) is wholly unsupported by any evidence of loss and/or damage to its property or possessions and (2) adds nothing to the analysis under Art. 8 ECHR. In those circumstances this has also not been addressed separately below.

Issue: Does the Equipment Interference Regime satisfy the requirements in Art. 8(2) that any interference be “in accordance with the law”

The test to be applied

146. The expression “in accordance with the law” requires:

“... firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law ...” (Weber, at §84.)

Domestic law

- 146A. It is denied that any carrying out of CNE operations by GCHQ pursuant to warrants/authorisations issued under s.5 and s.7 of the ISA, prior to the coming into force of the Serious Crime Act 2015 (which amended the CMA), was not in accordance with domestic law, whether as alleged in §37 and §41B(a) of Privacy’s Amended Grounds, or at all. Without prejudice to the generality of that denial, the Respondents’ position can be summarised as follows:

a) In enacting the ISA in 1994, after the coming into force of the CMA in

1990, Parliament made specific provision for the Intelligence Services, including GCHQ, to conduct activities which might otherwise be unlawful (whether under criminal or civil law), where the activity was authorised by s. 5 warrants or s. 7 authorisations. That is clear from the express language of the ISA and, in particular at s.5(1) and s.7(1)-(2), as set out at §47 and §55 above.

- b) As regards GCHQ's activities, Parliament was also clear when enacting the ISA that such activities should include the monitoring or interference with any equipment producing electromagnetic, acoustic and other emissions, as expressly stated to be part of GCHQ's statutory functions in s. 3(1)(a) of the ISA which language plainly includes interferences which would otherwise constitute an offence eg. of impairing the operation of a computer under s.3 of the CMA.
- c) Consequently the specific statutory scheme in the ISA is structured such that both s.5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that they are not civilly or criminally liable for such interferences, including under the CMA.
- d) S.10 of the CMA (prior to being amended on 3 May 2015) did not have the effect that only lesser interferences, amounting to a breach of s.1 of the CMA, could be authorised, including under the ISA or RIPA, as alleged in §37 and §41B(a) of Privacy's Amended Grounds. That section was directed at "certain law enforcement powers" (see the title to s. 10) i.e. powers of inspection, search or seizure (eg. by the police) and it did not purport to set out the circumstances in which, what would otherwise be offences under the CMA, might be authorised eg. by the Intelligence Services when exercising their statutory functions including in the interests of national security and the prevention and detection of serious crime.
- e) The amendments to s.10 CMA were clarificatory only, as is evident from the explanatory notes to that section, set out at §37C of Privacy's Amended Grounds and as made clear in the Home Office Fact Sheet to the Serious Crime Act 2015 (Part 2: Computer Misuse) and the Home Office Circular, both dated March 2015, which stated as follows:

"Section 44 clarifies the savings provision at section 10 of the 1990 Act and is intended to remove any ambiguity for the lawful use of powers to investigate crime (for example under Part 3 of the Police Act 1997) and the interaction of those powers with the offences in the 1990 Act. The changes do not extend law enforcement agencies' powers but merely clarify the use of existing powers (derived from other enactments, wherever exercised) in the context of the offences in the 1990 Act." (Home Office Fact Sheet)

"Section 44 clarifies section 10 of the CMA. Section 10 of the CMA

contained a saving provision whereby criminal investigations by law enforcement agencies did not fall foul of the offences in the Act. However, section 10 pre-dates a number of the powers, warranting and oversight arrangements on which law enforcement now rely to conduct investigations, such as those in Part 3 of the Police Act 1997. The changes do not extend law enforcement agencies' powers but merely clarify the use of the existing powers (derived from other enactments, wherever exercised) in the context of the offences in the CMA." (Home Office Circular)

- f) The interpretation contended for by the Claimants would lead to the absurd result that the authorisation mechanisms in the ISA could have no legal effect unless there was an express savings provision in each relevant piece of legislation (whether governing criminal or civil liability), making clear that it was without prejudice to powers set out in any other enactment. That is manifestly inconsistent with the scheme of the ISA. It also elevates the status of savings provisions eg. in the CMA, beyond that which is tenable. As has been recognised in the case law, savings provisions are a frequently unreliable guide to the provisions to which they attach, since savings provisions "are often included by way of reassurance, for the avoidance of doubt or for an abundance of caution"³³.

146B. In the premises the submissions at §37 and §41B(a) of Privacy's Amended Grounds are wrong in law and misconceived.

146C. As to §§37D, 37F, 41B(b) and 47A of Privacy's Amended Grounds:

- a) The Respondents confirm that, as a matter of practice, any CNE activities carried out abroad, or over a foreign computer, even if the relevant user is located in the United Kingdom, would be authorised by an authorisation issued under section 7 ISA.
- b) The very purpose of section 7 of the ISA is to provide for the granting of authorisations in respect of any act done outside the British Islands, where otherwise a person would be liable under the criminal or civil law of the UK. In addition, section 7(9) of the ISA makes clear that such authorisations can relate to an act which is done in the British Islands, but which is or is intended to be done in relation to apparatus that is believed to be outside the British Islands.
- c) In those circumstances any questions as to the applicability and/or effect of section 31 of the Criminal Justice Act 1948 ('the CIA') are irrelevant in these proceedings.
- d) Without prejudice to that, the Respondents do not accept that section 31 of the CIA extends the scope of the territorial jurisdiction provisions in the CMA (see §37F of Privacy's Amended Grounds), nor

³³ See Lord Simon of Glaisdale in *Ealing London Borough Council v Race Relations Board* [1972] AC 342 at 363.

are the broad assertions in §41B(b) of Privacy's Amended Grounds accepted as an accurate statement of the law. In particular:

- i) It is denied that the offences under the CMA are capable of being transposed under the CIA, in circumstances where the CMA makes clear what significant link with domestic jurisdiction is necessary in order for any offence to be committed. If a significant link with jurisdiction is not, in fact, present, it is denied that an offence will have been committed, whether under the CMA or the CIA.
- ii) Further and/or alternatively and without prejudice to subparagraph (i) above, even if the CIA did apply, the question whether there was any liability under section 31 of the CIA, read with the CMA, would depend upon the specific circumstances in question including, *inter alia*, the answers to the following key questions:
 - (1) Whether the offence was contrary to the laws of the foreign country i.e. it would only be where the Crown Servant commits an offence contrary to the laws of the foreign country and which would be indictable in England, that section 31 of the CIA could apply; and
 - (2) Whether the offence was committed in a "foreign country" which bears a special meaning derived from the British Nationality Act 1948, which was repealed in part and replaced with the British Nationality Act 1981 and which means that section 31 of the CIA does not apply to (a) Commonwealth countries, (b) the Republic of Ireland and (c) British overseas territories.

146D. As to paragraph 41C of Privacy's Amended Grounds:

1. The references to sections 5 and 7 ISA 1994 are noted.
2. Insofar as necessary, the interpretation of the said provisions will be the subject of submission in due course.
3. The meaning of the terms "thematic" and "class" as used by Privacy are not understood in this context. Neither term forms part of the statutory requirements for the issue of a warrant under section 5.
 - a. If and insofar as the term "thematic" used by Privacy refers to the usage by the Intelligence Services Commissioner in his 2014 Report at page 18, the following matters are noted:
 - i. As set out at paragraph 47 above, section 5(1) provides: "No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section." That provision does not delimit the scope of a warrant to any single piece of property or single instance or method of entry on to or interference with property or wireless telegraphy.

- ii. By section 5(2) the Secretary of State may, on an application by GCHQ, issue a section 5 warrant authorising "the taking, subject to subsection (3) ..., of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified". If and insofar as action and/or property and/or wireless telegraphy is specified in a section 5 warrant, the warrant will be valid as regards that specification.
 - iii. Whether action and/or any property and/or wireless telegraphy is "specified" in a warrant will depend upon the words used in the particular warrant.
 - iv. If and to the extent that it is the Claimant's case that the terms "any property so specified" in section 5(2) are to be read as precluding the Secretary of State from issuing a warrant save in relation to a particular operation against a particular piece of property, that is denied.
 - v. For the avoidance of doubt, "property" can be "specified" in a section 5 warrant by description. Such description may encompass more than one particular location or item of property.
- b. The term "class" is not used by Commissioner in his Report in connection with section 5 warrants. It is a term used by him in connection with section 7 authorisations.
4. It is denied that warrants issued (and acts authorising warrants) under section 5 ISA 1994 were or are unlawful. It is averred that the Secretary of State can only sign a warrant if satisfied that the activity thereby authorised is necessary and proportionate.

146E. Paragraph 41D of Privacy's Amended Grounds is denied. Insofar as necessary, the interpretation of sections 5 and 7 ISA 1994 (and the significance or otherwise of the wording of ss.5(3) and (3A)) will be the subject of submission in due course.

146F. To the extent that paragraph 41E of Privacy's Amended Grounds is understood it is denied:

- a. The nature or type of the alleged interference with copyright is unduly vague and inadequately pleaded (by reference to other allegations made or otherwise).
- b. Further, the relevance of Directive 2001/29 is not understood. The relevant law of copyright is the domestic law of England and Wales and no breach thereof is alleged. It is not contended that the United Kingdom has failed to implement Directive 2001/29 in domestic law. For the avoidance of doubt, it is noted that Directive 2001/29 was implemented in the United Kingdom in particular in the Copyright Designs and Patents Act 1988 (as amended).
- c. Further or alternatively, insofar as it is relevant, it is denied that (i) the actions of the Defendant pursuant to the protection of national

security interfere with any rights protected under Directive 2001/29 and/or (ii) any interference with such rights by the actions of the Defendants is unlawful or disproportionate.

146G. Paragraph 41F of Privacy's Amended Grounds and its relevance is denied. Submissions on the nature, terms and effect of the judgment in Case C-293/12 will be made as necessary in due course. For the avoidance of doubt, the said judgment, inter alia, was not concerned with copyright, did not consider standards required for derogations under Directive 2001/29 (the relevance of which is not understood – see paragraph 146F(b) above) and did not purport to lay down “the standard required to justify a derogation from EU law rights” whether in relation to “surveillance” or otherwise.

Articles 8 and 10 ECHR

147. In relation to ‘foreseeability’ in this context, the essential test, as recognised in §68 of *Malone v. UK* (1984) 7 EHRR 14 and in §37 and §118 of the *Liberty/Privacy* judgment, is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity “to give the individual adequate protection against arbitrary interference”. As the Grand Chamber recently confirmed in the eavesdropping case of *Bykov v. Russia*, appl. no. 4378/02, judgment of 21 January 2009, this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §78, as quoted at §37 of the *Liberty/Privacy* judgment).³⁴

148. Consequently the key question when considering whether the Equipment Interference Regime satisfies the “in accordance with the law” test under Art. 8(2) is whether there are:

“...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.” (see §125 of the Liberty/Privacy judgment)

149. As noted by the Tribunal in the *Liberty/Privacy* judgment, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §38-40 and §137). That was made very clear by the Strasbourg Court at §§67-68 of *Malone* and in *Leander v Sweden* [1987] 9 EHRR 433 at §51 and *Esbeester v UK* [1994] 18 EHRR CD 72, as quoted at §§38-39 of the Tribunal’s judgment in *Liberty/Privacy*.

³⁴The “necessity” requirement also calls for adequate and effective safeguards against abuse. But the Tribunal is sufficient for this purpose: §59 of *Rotaru v. Romania* (2000) 8 BHRC 449 (“effective supervision ... should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure ...”). *A fortiori*, the combination of the Tribunal, the ISC and the Commissioner satisfies this aspect of the “necessity” requirement.

150. Thus, as held by the Tribunal in the *British Irish Rights Watch* case dated 9 December 2004 (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87):

"foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security..."
(§38)

151. Consequently the national security context and the particular national security justification for the activity/conduct which is impugned is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the *Liberty/Privacy* judgment).
152. Moreover, the ECtHR has consistently recognised that the foreseeability requirement "cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly": *Malone v. UK* (1984) 7 EHRR14, at §67; *Leander v. Sweden* at §51; and *Weber*, at §93.
153. As to the procedures and safeguards which are applied, two important points should be noted.
154. First it is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* and in *Bykov* at §78 and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy*.
155. Secondly it is permissible for the Tribunal to consider rules, requirements or arrangements which are "below the waterline" i.e. which are not publicly accessible. In *Liberty/Privacy* the Tribunal came to the clear conclusion that it is "not necessary that the precise details of all of the safeguards should be published, or contained in legislation, delegated or otherwise" (§122), in order to satisfy the "in accordance with the law" requirement and that the Tribunal could permissibly consider the "below the waterline" rules, requirements or arrangements when assessing the ECHR compatibility of the regime (see §§50, 55, 118, 120 and 139 of the judgment). At §129 of the judgment in *Liberty/Privacy* the Tribunal stated:

"Particularly in the field of national security, undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise...This is particularly so where:

- (i) *The Code...itself refers to a number of arrangements not contained in the Code...*
- (ii) *There is a system of oversight, which the ECHR has approved, which ensures that such arrangements are kept under constant review."*

156. Although these conclusions were reached in the context of the s. 8(4) RIPA interception regime, they are equally applicable to the equipment regime where the relevant IE Code and Property Code both refer expressly to undisclosed statutory “arrangements” under the ISA (see eg. §1.3 of the IE Code and §7.38 and §9.7 of the Property Code) and where there is similar oversight by the Intelligence Services Commissioner.
157. In terms of oversight mechanisms, it is important to note the extent to which the Tribunal in *Liberty/Privacy* placed reliance on these mechanisms when concluding that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8(2) compliant. Thus the Tribunal highlighted the advantages of the Tribunal as an oversight mechanism at §46 and the importance of these oversight mechanisms in the s. 8(4) regime at §122. Therefore, as the ECtHR recognised in §95 of *Weber*, account should be taken of all the relevant circumstances, including:

“the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ...” (*Association for European Integration and Human Rights v. Bulgaria*, Appl. no. 62540/00, judgment of 28 June 2007, at §77.)

Application to the Equipment Interference Regime

158. In terms of the criticisms which are made of the legal framework in the Claimants’ Grounds, the Respondents make the following six points in this response and pending further clarification of the Claimants’ case in due course.
159. First, it is not accepted, even on the basis of the factual assertions made in the Grounds (which are neither confirmed nor denied), that such activities are factually or legally more intrusive than other forms of surveillance or data-gathering, including the interception of communications (see §§42-46 of the Privacy Grounds and §§55-57 of the Greennet Grounds).
160. The ECtHR has expressly referred to the fact that “rather strict standards” apply in the interception context, but do not necessarily apply in other intelligence-gathering contexts: *Uzun v. Germany* (2011) 53 EHRR 24, at §66 and *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, per Lord Carswell at §85. There is no factual or legal justification for asserting that an even stricter set of standards ought to apply to equipment interference activities, over and above those which would apply eg. to an interception case.
161. Secondly, contrary to the assertion made in the Grounds, there is a clear legal framework governing any equipment interference activities, as set out in detail earlier in this Response. The availability of warrants under s. 5 and authorisations under s. 7 of the ISA, do provide a firm legal framework which is supplemented in important respects by the CMA, HRA, the DPA, the OSA, the IE Code, GCHQ’s internal arrangements and the Property Code. That statutory scheme, in common with the interception regime in RIPA, makes

certain activities an offence (as is the case eg. in s. 1 of RIPA which makes it an offence, without lawful authority to intercept certain communications) but is coupled with a regime for the issuing of warrants/authorisations which render the activity lawful if strict conditions are satisfied. The suggestion that the availability of a warrant under the ISA "simply cancels any unlawfulness" is a misrepresentation and an over-simplification of the statutory scheme and the safeguards which are inherent within it.

162. The Equipment Interference regime is therefore "accessible" and has a basis in domestic law, in that it consists of provisions in primary legislation and in relevant Codes and also in relevant internal arrangements/safeguards which are applied by GCHQ. The Claimants' argument that there is no relevant legal regime that regulates the circumstances in which and the conditions in which GCHQ may interfere with equipment is therefore untenable.
163. Thirdly it is wrong to suggest that there is no Code of Practice governing equipment interference. As has been set out in detail above, there has always been a Code which governed property interference (including equipment interference) and there is now a bespoke Code, the EI Code, which contains important safeguards including, *inter alia*:
- (a) Detailed guidance on the requirement of proportionality and the considerations which apply in the equipment interference context, including issues such as collateral intrusion and the need to consider less intrusive alternatives (Chapter 2);
 - (b) Guidance on the frequency of reviews, particularly where there is a high level of intrusion into private life or significant collateral intrusion or confidential information is likely to be obtained (Chapter 2 at §§2.13-2.15);
 - (c) Best practice guidance on applications for warrants/authorisations (§§2.16-2.17);
 - (d) Special considerations which should apply to legally privileged and confidential information (Chapter 3);
 - (e) Detailed and comprehensive procedures for the authorisation of both s. 5 and s. 7 ISA equipment interference activity (see Chapters 4 and 7);
 - (f) Important record keeping requirements in respect of any equipment interference (Chapter 5);
 - (g) Comprehensive safeguards and guidance as regards the processing, retention, disclosure, deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant, which mirror similar safeguards applied as part of the interception regime pursuant to s. 15 of RIPA (Chapter 6)..

In addition, GCHQ's internal arrangements contain safeguards as set out at §§99B-99ZS above.

164. Fourthly it is submitted that the Equipment Interference Regime does indicate the scope of any discretion and the manner of its exercise with sufficient clarity "to give the individual adequate protection against arbitrary interference" (*Malone*, at §68). In overview:

- (a) The regime is sufficiently clear as regards the circumstances in which there can be interferences with equipment. Any warrants/authorisations in respect of equipment interference by the Intelligence Services can only be issued if clear statutory criteria are satisfied, including the requirements of necessity and proportionality and such permission can only be given by the Secretary of State personally, save in an urgent case.
 - (b) The regime is similarly sufficiently clear as regards the subsequent handling, use and possible onward disclosure of any information so obtained. In this regard the ISA must be read in conjunction with other important safeguards in the CTA, the DPA, the HRA, the OSA and the Codes.
165. Further, if some version of the list of "safeguards" in e.g. §95 of *Weber* applies to the Equipment Interference Regime, the present regime satisfies the requirements for such "safeguards", insofar as it is feasible to do so.
- (a) The first and second requirements in *Weber* i.e. the "offences" which may give rise to a warrant/authorisation and the categories of people liable to be involved, are clearly satisfied by s. 5 and s.7 of the ISA, as read, in particular, with §1.6, §§4.1-4.4 and §7.8 of the IE Code. It is also to be noted that the term "national security" is a sufficient description in the ISA (see §116 of the *Liberty/Privacy* judgment).
 - (b) The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are addressed, in particular, in the ISA, the CTA, the DPA, the HRA, the OSA and in Chapters 2, 4, 6 and 7 of the IE Code and GCHQ's internal arrangements. In particular:
 - (a) The ISA makes sufficient provision for the duration of s.5/s.7 warrants/authorisations and the circumstances in which they can be renewed or should be cancelled. In addition the IE Code contains important provisions on reviewing warrants and the frequency of reviews (see §2.13-2.15).
 - (b) There are detailed safeguards which apply which mirror the safeguards in s.15 of RIPA in the interception regime, as regards the handling, dissemination, copying, storage, destruction and security arrangements for information obtained as a result of equipment interference (see in particular Chapter 6 of the IE Code). Further GCHQ must ensure that there are internal arrangements in force, which are approved by the Secretary of State, for securing that the requirements set out in Chapter 6 of the IE Code are satisfied in relation to all information obtained by equipment interference (see §6.4 of the IE Code) and these internal arrangements should be made available to the Commissioner (see §6.5 of the IE Code).

- (c) Any information emanating from equipment interference can be used by GCHQ only in accordance with s.19(2) of the CTA as read with the statutory definition of GCHQ's functions (in s. 3 of the ISA) and only insofar as that is proportionate under s.6(1) of the HRA;
 - (d) In addition any disclosure of such information must satisfy the constraints imposed in s. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA;
 - (e) There is also the requirement for statutory arrangements to be in place, by reference, in particular, to the ISA (s. 4(2)(a) and the EI Code itself makes reference to such arrangements at §1.3;
 - (f) Any disclosure eg. deliberately in breach of the "arrangements" for which provision is made in s.4(2)(a) of the ISA would be criminal under s.1(1) of the OSA.
166. Fifthly the Tribunal can take into account the "*below the waterline*" rules, requirements and arrangements which regulate any equipment interference activities which may be conducted by GCHQ. These have been addressed above (at §§99B-99ZS) and separately in GCHQ's Closed Response to the complaints. Those rules, requirements and arrangements fully support the contentions set out above about the lawfulness of the regime.
167. Finally there are important oversight mechanisms which are relevant to the Article 8(2) compatibility of the regime including the Tribunal, the ISC and the Intelligence Services Commissioner. These oversight mechanisms are centrally relevant to the question whether the regime provides for adequate protection against abuse. The combination of these oversight mechanisms is a very important safeguard in the context of the Art 8(2) compatibility of the regime.
168. In conclusion the Equipment Interference Regime is sufficiently accessible and "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2).
169. In relation to paragraph 52A of Privacy's Amended Grounds paragraphs 146F-G above are repeated.

SUGGESTED DIRECTIONS

- ~~170. The Respondents invite the Tribunal to make the following directions, prior to any directions hearing:~~
- ~~(a) Within 21 days of service of this Response, the Claimants shall confirm in writing whether the Issues for the Legal Issues Hearing~~

~~that are identified in this Response are agreed and, to the extent that they are not, shall set out the pure issues of law which they propose should be determined at that hearing. The Claimants to be at liberty to file Replies by the same date.~~

~~(b) Within 21 days thereafter the parties to file and serve their suggested directions for the management of the Claims up to and including the Legal Issues Hearing.~~

~~171. The Respondents would be content for the Tribunal to hold a public *inter partes* directions hearing to determine the procedure to be adopted in the two Claims. They respectfully submit that any directions hearing be listed on a date when all counsel are able to attend, given the specialist nature of the proceedings. At any directions hearing, the Respondents will propose that the two Claims be formally joined.~~

6 February 2015

28 May 2015

25 September 2015

13 November 2015

JAMES EADIE QC
DANIEL BEARD QC
KATE GRANGE
RICHARD O'BRIEN

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

RESPONDENTS' RESPONSE TO THE GREENNET CLAIMANTS' REQUEST FOR
FURTHER INFORMATION DATED 6 MARCH 2015

This is the Respondents' Response to the Greennet Claimants' Request for Further Information dated 6 March 2015

Of paragraph 3

1. Is it the Respondents' case that the Equipment Interference Regime was compatible with Articles 8, 10 or Article 1 of the First Protocol prior to the publication of the draft Equipment Interference Code of Practice? If so, please explain why.

Yes it is the Respondent's position that the Equipment Interference Regime was compatible with Articles 8, 10 and Article 1 of the First Protocol prior to the publication of the draft Equipment Interference Code of Practice.

In summary it is the Respondents' position that the combination of:

- (a) the Intelligence Services Act 1994 ("the ISA"), (and, in particular, ss. 3, 5 and 7 of that Act) (as read with the Counter-Terrorism Act 2008 ("the CTA") and the Computer Misuse Act 1990 ("the CMA")) (see §§ 36-64 of the Respondents' Open Response); and
- (b) the Human Rights Act 1998 ("the HRA") (see §103-107 of the Respondents' Open Response); and
- (c) the Data Protection Act 1998 ("the DPA") (see §108-110 of the Respondents' Open Response); and
- (d) the Official Secrets Act 1989 ("the OSA") (see §111-112 of the Respondents' Open Response); and
- (e) the Covert Surveillance and Property Interference Code ("the Property Code") (see §§101 of the Respondents' Open Response) (which first came into force in 2002 and which was subsequently amended in 2010 and 2014); and
- (f) the oversight mechanisms set out at §§113-142 of the Respondents' Open Response; and
- (g) the 'below the waterline safeguards' referred to at §166 of the Respondents' Open Response and addressed separately in the Respondents' Closed Response;

are such that the regime was compatible with Articles 8, 10 and Article 1 of the First Protocol, including the "in accordance with the law" requirement under Article 8(2), as summarised at §125 of the Tribunal's judgment in *Liberty/Privacy* dated 5 December 2014.

The Respondents reserve the right to set out their position in further detail in a skeleton argument in due course.

Of Paragraph 21

"CNE operations vary in complexity. At the lower end of the scale, an individual may use someone's login credentials to gain access to information. More complex operations may involve exploiting vulnerabilities in software in order to gain control of devices or networks to remotely extract information, monitor the user of the device or take control of the device or network... CNE... operations may also be carried out lawfully by certain public authorities"

2. Has the fact that UK public authorities:
- a. carry out CNE operations;
 - b. carry out CNE operations involving using someone's login credentials;
 - c. carry out CNE operations involving exploiting vulnerabilities in software in order to gain control of devices;
 - d. carry out CNE operations involving exploiting vulnerabilities in software in order to gain control of networks;
 - e. carry out CNE operations in order to remotely extract information;
- previously been disclosed to the public? If so, for each of subparagraphs a to e above, when and how?

Paragraph 21 provides examples of the sorts of activities which may comprise CNE, whether those activities are conducted by criminals or hackers or lawfully by public authorities. However the Respondents can neither confirm nor deny whether public authorities (generally so defined) have, in fact, carried out such operations.

In terms of the Intelligence Services, to the best of the Respondents' knowledge, no public statements have been made about the use of CNE as a specific investigative technique, prior to publication of the EI Code - see the Consultation Paper dated 6 February 2015 on 'Equipment Interference and Interception of Communications Codes of Practice' and see the Written Ministerial Statement dated 6 February 2015 which accompanied the publication of the Codes. However the concept of property interference by the Intelligence Services (which would implicitly include interference with computer equipment) has been in the public domain for some considerable time and, for example, is addressed in the ISA 1994 and in the Property Code which was first published in 2002.

Of Footnote 17

"By section 17(5) of the CMA "Access of any kind by any person to any program or data held in a computer is unauthorised if - (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled" (NB. This subsection is subject to section 10 which contains a saving in respect of certain law enforcement powers)."

3. This footnote is the only pleading in response to paragraph 37 of the claim by Privacy International. In paragraph 37, Privacy International note that the saving in section 10 does not apply to an offence under section 3(1) of the CMA 1990. Therefore, any GCHQ activities that impair the operation of a computer, for example by leaving it vulnerable to future exploitation, or which use up its battery or slow it down or harm its operation in any other way are prima facie unlawful. Do the Respondents admit or deny paragraph 37 of the claim? If paragraph 37 is denied, please set out why.

It is admitted that section 10 of the CMA 1990 applies to section 1(1) of that Act and not section 3(1) as the express language of the Act makes clear.

As to the specific allegations in paragraph 37 about the lawfulness of GCHQ activities, nothing further can be said in Open in response to those allegations.

Of Paragraph 45

"Save in respect of certain offences (i.e. under s. 2 of the CMA), at least one significant link with domestic jurisdiction must exist in the circumstances of the case for an offence to be committed."

4. Do the Respondents accept that pursuant to section 31 of the Criminal Justice Act 1948, interference with the operation of a computer by a Crown servant acting in the course of his employment, wherever in the world the computer or the Crown servant are located, is a prima facie criminal breach of the CMA 1990, read with section 31 of the 1948 Act? If not, please set out why not.

The Respondents are not prepared to make an admission about the application of the Computer Misuse Act 1990, as read with section 31 of the Criminal Justice Act 1948 ('CJA 1948'), on the basis of such a generalised proposition.

The question whether an offence has been committed will depend on all the facts of each individual case, including, *inter alia*, whether a significant link with domestic jurisdiction exists for an offence to be committed under the CMA (for which s.5 of the CMA provides exhaustive definitions) and whether, under the CJA 1948 an offence has been committed "in a foreign country" by a Crown servant when acting or purporting to act in the course of his employment, which, if committed in England, would be punishable on indictment, as if the offence had been committed in England.

Of Paragraph 66

"Whilst the Code is currently in draft, as set out in the Written Ministerial Statement which accompanied its publication, it reflects the current safeguards applied by the relevant Agencies, including GCHQ. The Agencies will continue to comply with the provisions of the draft Code throughout the consultation period and until the Code is formally brought into force. Consequently GCHQ can confirm that it complies with all aspects of the EI Code and can also confirm that it fully reflects the practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by GCHQ."

5. Why was the EI Code created?

The Respondents do not understand the relevance of this question to the issues in dispute in these proceedings and, in particular, whether the regime is compatible with Articles 8, 10 and Article 1 of the First Protocol to the ECHR.

6. Please provide a copy of any and all versions of the procedures referred to, any documents evidencing them (including any training manuals used in relation to them), and any internal reports, audits or investigations into compliance with those procedures. Please also identify the date on which each such procedure was introduced.

The Respondents can confirm that relevant versions of the procedures have been in place since at least 13 May 2013 (i.e. one year prior to issue of these complaints) and have been subject to regular review.

However the Respondents are unable to provide any further information because to do so would be damaging to the public interest or prejudicial to national security, the prevention or detection of serious crime and the continued discharge of the functions of the intelligence services (see Rule 6(1) of the Investigatory Powers Tribunal Rules and see, by analogy, §§55-61 and §100 of the witness statement of Charles Farr dated 16 May 2014 served in the *Liberty/Privacy* proceedings.).

7. Please provide a copy of any documents evidencing any and all versions of the practices and safeguards referred to (including any training manuals used in relation to them), and any internal reports, audits or investigations into compliance with those practices and safeguards. Please also identify the date on which each such practice or safeguard was introduced.

See answer to question 6 above.

8. If any practices, procedures or safeguards which have been in force at any point since 13 May 2013 (i.e. one year prior to the issue of Case No IPT 14/85/CH) have since been amended or repealed, please provide the information and documents requested at paragraphs 6 and 7 above in respect of each of those practices, procedures or safeguards, and identify (i) the date on which they were amended or repealed and (ii) the reason why they were amended or repealed.

See answer to question 6 above.

9. Paragraphs 3.9-3.19 of the draft EI Code contain safeguards relating to legal professional privilege. Is it alleged that these are procedures which "GCHQ has always applied to any equipment interference activities"? If so, when were such procedures introduced? If they have been amended since 13 May 2013, please provide the information requested at paragraphs 6 and 7 above in respect of the previous version or versions, and identify (i) the date on which they were amended and (ii) the reason why they were amended.

Without prejudice to the fact that the complaints which have been made by the Claimants do not raise any questions as to the obtaining and/or handling of LPP material, GCHQ can confirm that the key safeguards in respect of LPP material set out in the EI Code have been applied by GCHQ to any EI activities, save that the safeguards at paragraph 3.18 were not previously part of GCHQ's practice or policy. However it is accepted that paragraphs 3.9-3.19 of the EI Code contain more detail on the safeguards for the use and handling of matters subject to LPP and in particular on the requirement for 'chinese wall' safeguards where there is eg. civil proceedings against the Agencies.

Of Paragraph 68

"To the extent that the EI Code overlaps with the guidance provided in the Covert Surveillance and Property Interference Revised Code of Practice issued in 2014 (see further below), the EI Code takes precedence, however the Intelligence Services must continue to comply with the 2014 Code in all other respects (see §1.2)."

10. Which provisions in the Covert Surveillance and Property Interference Revised Code of Practice are disapplied in favour of the provisions of the EI Code, and in what circumstances?

The EI Code provides standalone guidance for any person conducting EI i.e. the EI Code entirely replaces the old Covert Surveillance and Property Interference Revised Code of Practice for any activity falling within the definition of EI. Paragraph 1.2 of the EI Code confirms that the Property Code will continue to apply to other property interference falling outside the definition of EI.

11. Was the position the same prior to the creation of the EI Code? If not, which provisions in the Covert Surveillance and Property Interference Revised Code or Practice were disapplied in favour of the "practices, procedures and safeguards" which GCHQ allegedly applied to equipment interference activities prior to releasing the draft Equipment Interference Code, and in what circumstances?

GCHQ can confirm that no provisions in the Property Code were disapplied in favour of its internal practices/procedures/safeguards.

Of Paragraph 69

"The EI Code also records the fact that there is a duty on the heads of the Intelligence Services to ensure that arrangements are in force to secure: (i) that no information is obtained by the Intelligence Services except so far as necessary for the proper discharge of their statutory functions; and (ii) that no information is disclosed except so far as is necessary for those functions [...]"

12. Do the Respondents rely for the purposes of these proceedings on any such arrangements?

Yes.

13. If so, please specify the arrangements and the dates on which they came into effect, and provide a copy of any documents which record or evidence them.

See the answer to question 6 above.

14. If any such arrangements have been in force at any point since 13 May 2013 (i.e. one year prior to the issue of Case No IPT 14/85/CH) but have since been amended or repealed, please provide the information and documents requested at paragraph 13 above in respect of each of those arrangements, and identify (i) the date on which they were amended or repealed and (ii) the reason why they were amended or repealed.

See the answer to question 6 above.

Of Paragraph 77

"where it is proposed to conduct equipment interference activity specifically against individuals who are not intelligence targets in their own right, interference with the equipment of such individuals should not be considered as collateral intrusion but rather as "intended intrusion"..."

15. In what circumstances is equipment interference activity conducted against individuals who are not intelligence targets in their own right?

The Respondents cannot confirm or deny whether equipment interference activity does or does not take place in particular operational contexts. However, the Respondents can give the example set out at paragraph 3.11 of the Property Code which states:

"Example: A law enforcement agency seeks to conduct a covert surveillance operation to establish the whereabouts of N in the interests of preventing a serious crime. It is proposed to conduct directed surveillance against P, who is an associate of N but who is not assessed to be involved in the crime, in order to establish the location of N. In this situation, P will be the subject of the directed surveillance authorisation and the authorising officer should consider the necessity and proportionality of conducting directed surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be

the case that directed surveillance of P will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the authorising officer."

16. Has GCHQ always treated interference with the equipment of individuals who are not intelligence targets in their own right as "intended intrusion" and not collateral intrusion?

Yes - GCHQ has always complied with the provisions of the Property Code.

17. What difference does it make to GCHQ's decision-making process to treat interference as "intended intrusion" rather than collateral intrusion?

Pursuant to Chapter 4 of the EI Code, it would affect the information which had to be provided with any warrant application by way of justification for such an operation (see paragraph 4.6 and the information checklist provided therein). In addition the EI Code specifically states at paragraph 2.12 that:

"Any such equipment interference activity should be carefully considered against the necessity and proportionality criteria as described above."

Of Paragraph 81

"Chapter 3 of the Code contains detailed provisions on legally privileged and confidential information which it is intended to obtain or which may have been obtained through equipment interference."

18. Is it the Respondents' case that the provisions in Chapter 3 of the draft EI Code concerning legally privileged information are compliant with Articles 8, 10 and Article 1 Protocol 1 ECHR?

The relevance of this question to the complaints raised by the Claimants is not understood. Neither of the complaints raise questions as to the obtaining or handling of LPP material. Without prejudice to that, the Respondents repeat the answer to question 9 above and will say the EI Code is compliant with Articles 8, 10 and Article 1 Protocol 1 of the ECHR.

19. Is it the Respondents' case that the "practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by GCHQ" concerning legally privileged information, which the EI Code "fully reflects", at all times complied with any or all of Articles 8, 10 or Article 1 Protocol 1 ECHR?

The relevance of this question to the complaints raised by the Claimants is not understood. Neither of the complaints raise questions as to the obtaining or handling of LPP material. Without prejudice to that, the Respondents repeat the answer to question 9 above.

Of Paragraph 90

"At §§6.4-6.5 the importance of these safeguards is emphasised, together with the need to ensure that each of the Intelligence Services has internal arrangements in force for securing that the safeguards

are satisfied, which arrangements should be made available to the Intelligence Services Commissioner."

20. Do the Respondents rely for the purposes of these proceedings on any such internal arrangements?

Yes.

21. If so, please specify the arrangements and the dates on which they came into effect, and provide a copy of any documents which record or evidence them.

See the answer to question 6 above.

22. If any such arrangements have been in force at any point since 13 May 2013 (i.e. one year prior to the issue of Case No IPT 14/85/CH) but have since been amended or repealed, please provide the information and documents requested at paragraph 13 above in respect of each of those arrangements, and identify (i) the date on which they were amended or repealed and (ii) the reason why they were amended or repealed.

See the answer to question 6 above.

23. Has the Commissioner approved these arrangements? If so, when?

To date, the main arrangements have been seen and reviewed by the Commissioner and he has raised no concerns. Further details will be provided in CLOSED. Pursuant to the EI Code (which was introduced in draft on 6 February 2015) these arrangements will be made available to the Intelligence Services Commissioner during his visits.

24. Does the substance of the arrangements that are or have been in place differ in any material respect from the content of the draft EI Code? If so, in what respect?

No.

This document was withdrawn on 5 April 2016.



Home Office

INTERCEPTION OF COMMUNICATIONS DRAFT Code of Practice

Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000

November 2015

archived

archived

6

6

This document was withdrawn on 5 April 2016.

Interception of Communications
DRAFT Code of Practice

Presented to Parliament pursuant to section 71(4) of the Regulation of Investigatory Powers Act 2000

November 2015



© Crown copyright 2015

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at RIPA@homeoffice.gsi.gov.uk

Print ISBN 9781474124751

Web ISBN 9781474124768

ID 14091502 11/15

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

archived

CONTENTS

1. General.....	3
2. Unlawful interception - criminal and civil offences	4
3. General rules on interception with a warrant	5
Necessity and proportionality.....	5
Meaning of "telecommunications service"	6
Implementation of warrants	7
Provision of reasonable assistance	7
Provision of interception capability	8
Duration of interception warrants.....	9
Stored communications	9
4. Special rules on interception with a warrant	10
Collateral intrusion.....	10
Confidential information.....	10
Communications subject to legal privilege.....	11
Communications involving confidential journalistic material, confidential personal information and communications between a Member of Parliament and another person on constituency business.....	14
5. Interception warrants (section 8(1)).....	16
Application for a section 8(1) warrant	16
Authorisation of a section 8(1) warrant.....	17
Urgent authorisation of a section 8(1) warrant.....	17
Format of a section 8(1) warrant.....	17
Modification of a section 8(1) warrant.....	18
Renewal of a section 8(1) warrant	19
Warrant cancellation.....	19
Records	19
6. Interception warrants (section 8(4))	21
Section 8(4) interception in practice	21
Definition of external communications	22
Intercepting non-external communications under section 8(4) warrants.....	22
Application for a section 8(4) warrant	22

Authorisation of a section 8(4) warrant.....	23
Urgent authorisation of a section 8(4) warrant.....	24
Format of a section 8(4) warrant.....	24
Modification of a section 8(4) warrant and/or certificate	24
Renewal of a section 8(4) warrant	25
Warrant cancellation.....	25
Records	26
7. Safeguards	27
The section 15 safeguards	27
Dissemination of intercepted material.....	28
Copying	28
Storage.....	28
Destruction	29
Personnel security	29
The section 16 safeguards	29
8. Disclosure to ensure fairness in criminal proceedings.....	32
Exclusion of matters from legal proceedings	32
Disclosure to a prosecutor.....	32
Disclosure to a judge	33
9. Interception without a warrant.....	34
Interception with the consent of both parties	34
Interception with the consent of one party	34
Interception for the purposes of a communication service provider.....	34
Lawful business practice	35
10. Oversight.....	36
11. Complaints.....	37
12. Rules for requesting and handling unanalysed intercepted communications from a foreign government.....	38
Application of this chapter.....	38
Requests for assistance other than in accordance with an international mutual assistance agreement	38
Safeguards applicable to the handling of unanalysed intercepted communications from a foreign government.....	39

1. General

- 1.1 This code of practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers Act 2000 ("RIPA"), amended in 2014 by the Data Retention and Investigatory Powers Act 2014 ("DRIPA")¹. It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. This code of practice is primarily intended for use by those public authorities listed in section 6(2) of RIPA. It will also allow postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.
- 1.2 RIPA provides that all codes of practice issued under section 71 are admissible as evidence in criminal and civil proceedings. If any provision of this code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal, or to one of the Commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account.
- 1.3 This version of the code replaces all previous versions of the code.

¹ The Government has committed to bring forward legislation relating to the security, intelligence and law enforcement agencies' use of investigatory powers and to have that legislation enacted before the sunset provision in the Data Retention and Investigatory Powers Act 2014 takes effect on 31 December 2016.

2. Unlawful interception - criminal and civil offences

- 2.1 Interception is lawful only in the limited circumstances set out in section 1(5) of RIPA.
- 2.2 Section 1(1) of RIPA makes it a criminal offence for a person intentionally, and without lawful authority, to intercept in the United Kingdom (UK) any communication in the course of its transmission if that communication is sent via a public postal service or a public telecommunication system. The penalty for unlawful interception is up to two years' imprisonment or a fine up to the statutory maximum.
- 2.3 Section 1(1A) enables the Interception of Communications Commissioner to serve a monetary penalty notice imposing a fine of up to £50,000 if he or she is satisfied that:
- A person has unlawfully intercepted a communication at a place in the UK;
 - The communication was intercepted in the course of its transmission by means of a public telecommunication system;
 - The person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might explain the interception concerned;
 - The person has not committed an offence under section 1(1) of RIPA (intentional unlawful interception).
- 2.4 Guidance on the administration of these sanctions is available on the Commissioner's website:
<http://www.ioccb-uk.info>
- 2.5 Section 1(2) of RIPA makes it a crime for a person intentionally and without lawful authority to intercept in the UK any communication in the course of its transmission by means of a private telecommunication system, unless, as set out at section 1(6), the person has a right to control the operation or the use of the system, or has the express or implied consent of such a person to make the interception.

3. General rules on interception with a warrant

- 3.1 Interception has lawful authority where it takes place in accordance with a warrant issued under section 5 of RIPA. Chapter 9 of this code deals with the circumstances in which interception is permitted without a warrant.
- 3.2 There are a limited number of persons who can make an application for an interception warrant, or an application can be made on their behalf. These are:
- The Director-General of the Security Service.
 - The Chief of the Secret Intelligence Service.
 - The Director of the Government Communications Headquarters (GCHQ).
 - The Director-General of the National Crime Agency (NCA handles interception on behalf of law enforcement bodies in England and Wales).
 - The Chief Constable of the Police Service of Scotland.
 - The Commissioner of the Police of the Metropolis (the Metropolitan Police Counter Terrorism Command handles interception on behalf of Counter Terrorism Units, Special Branches and some police force specialist units in England and Wales).
 - The Chief Constable of the Police Service of Northern Ireland.
 - The Commissioners of Her Majesty's Revenue & Customs (HMRC).
 - The Chief of Defence Intelligence.
 - A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the UK.
- 3.3 Any application made on behalf of one of the above must be made by a person holding office under the Crown.
- 3.4 All interception warrants are issued by the Secretary of State.² Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.

Necessity and proportionality

- 3.5 Obtaining a warrant under RIPA will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR) if it is necessary and proportionate for the interception to take place. RIPA recognises this by

² Interception warrants may be issued on "serious crime" grounds by Scottish ministers, by virtue of arrangements under the Scotland Act 1998. In this code references to the "Secretary of State" should be read as including Scottish ministers where appropriate. The functions of the Scottish ministers also cover renewal and cancellation arrangements.

first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds:

- In the interests of national security;
- To prevent or detect serious crime;
- To safeguard the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

3.6 These purposes are set out in section 5(3) of RIPA. The Secretary of State must also believe that the interception is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.7 The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed interference against what is sought to be achieved;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought.

Meaning of "telecommunications service"

3.8 Section 2 of RIPA defines "telecommunication service" as any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system. Section 2(8A) of RIPA makes clear that any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system are included within the meaning of "telecommunications service". Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition. The definition of "telecommunications service" in RIPA is intentionally broad so that it remains relevant for new technologies.

Implementation of warrants

- 3.9 After a warrant has been issued it will be forwarded to the person to whom it is addressed - in practice the intercepting agency which submitted the application. Section 11 of RIPA then permits the intercepting agency to carry out the interception, or to require the assistance of other persons in giving effect to the warrant. A warrant may be served on any person who is required to provide assistance in relation to that warrant.
- 3.10 Where a copy of an interception warrant has been served on anyone providing a postal service or a public telecommunications service, or who has control of a telecommunication system in the UK, that person is under a duty to take all such steps for giving effect to the warrant as are notified to him or her by or on behalf of the person to whom the warrant is addressed. This applies to any company offering services to customers in the UK, irrespective of where the company is based. Section 11 also sets out the means by which that duty may be enforced.
- 3.11 Section 11(2B) of RIPA provides that service of a copy of a warrant on a person outside the UK may (in addition to electronic or other means of service) be effected in any of the following ways:
- By serving it at the person's principal office within the UK or, if the person does not have an office in the UK, at any place in the UK where the person carries on business or conducts activities;
 - At an address in the UK specified by the person;
 - By making it available for inspection at a place in the UK (if neither of the above two methods are reasonably practicable).

Provision of reasonable assistance

- 3.12 Any person providing a postal service or a public telecommunications service, or who has control of a telecommunications system in the UK, (referred to as communications service providers (CSPs) in this code) may be required to provide assistance in giving effect to an interception warrant. RIPA places a requirement on CSPs to take all such steps for giving effect to the warrant as are notified to them (section 11(4) of RIPA). But the steps which may be required are limited to those which it is reasonably practicable to take (section 11(5)). When considering this test, section 11(5)(a) specifies that regard must be had to any requirements or restrictions under the law of the country where the CSP is based that are relevant to the taking of those steps. It also makes clear the expectation that CSPs will seek to find ways to comply without giving rise to conflict of laws. What is reasonably practicable should be agreed after consultation between the CSP and the Government. If no agreement can be reached it will be for the Secretary of State to decide whether to press forward with civil proceedings. Criminal proceedings may also be instituted by, or with the consent of, the Director of Public Prosecutions.

- 3.13 Where the intercepting agency requires the assistance of a CSP in order to implement a warrant, it should provide the following to the CSP:
- A copy of the signed and dated warrant instrument;
 - The schedule setting out the numbers, addresses or other factors identifying the communications to be intercepted by the CSP for warrants issued in accordance with section 8(1);
 - A covering document from the intercepting agency (or the person acting on behalf of the agency) requiring the assistance of the CSP and specifying any other details regarding the means of interception and delivery as may be necessary. Contact details with respect to the intercepting agency will either be provided in this covering document or will be available in the handbook provided to all CSPs who maintain an interception capability.

Provision of interception capability

- 3.14 Persons who provide a public postal or telecommunications service, or plan to do so, may be required to provide a permanent interception capability (under section 12 of RIPA). The obligations the Secretary of State considers reasonable to impose on such persons to ensure they have a capability are set out in an order made by the Secretary of State and approved by Parliament³. Section 12(3A) of RIPA provides for the Secretary of State to serve a notice on a company located outside the UK but providing telecommunications services to customers within the UK, setting out the steps they must take to ensure they can meet these obligations. The Government must seek to consult with the CSP over the content of a notice before it is served.
- 3.15 Section 12(3B) of RIPA provides that where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the person:
- By delivering it to the person's principal office within the UK or, if the person does not have an office in the UK, to any place in the UK where the person carries on business or conducts activities;
 - At an address in the UK specified by the person.
- 3.16 When served with a notice, a CSP, if it feels it unreasonable, may refer that notice to the Technical Advisory Board (TAB) to consider the reasonableness of the technical requirements that are being sought and the financial consequences. Details of how to submit a notice to the TAB will be provided either before or at the time the notice is served.
- 3.17 Any CSP obliged to maintain a permanent interception capability will be provided with a handbook which will contain the basic information they require to respond to requests for reasonable assistance for the interception of communications.

³ Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 - <http://www.legislation.gov.uk/uksi/2002/1931>

Duration of interception warrants

- 3.18 Interception warrants issued on serious crime grounds are valid for an initial period of three months. Interception warrants issued on national security/economic well-being of the UK grounds are valid for an initial period of six months. A warrant issued under the urgency procedure (on any grounds) is valid for five working days following the date of issue unless renewed by the Secretary of State.
- 3.19 Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/ economic well-being of the UK grounds are valid for a further period of six months. These dates run from the date on the renewal instrument.
- 3.20 Where modifications to an interception warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification instrument expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.
- 3.21 Where a change in circumstance leads the intercepting agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

Stored communications

- 3.22 Section 2(7) of RIPA defines a communication in the course of its transmission as including any time when the communication is being stored on the communication system in such a way as to enable the intended recipient to collect it or otherwise have access to it. Making the contents of a communication stored in this way available to a person other than the sender or intended recipient therefore constitutes interception. A communication remains in the course of its transmission regardless of whether the communication has previously been read, viewed or listened to. A communication stored in this way remains in the course of its transmission.
- 3.23 Stored communications may also be accessed by means other than a warrant (see chapter 9). For example, if a communication has been stored on a communication system it may be obtained with lawful authority by means of an existing statutory power such as a production order (under the Police and Criminal Evidence Act 1984⁴) or a search warrant. A production order is an order from a circuit judge⁵, who must be satisfied that i) an indictable offence has been committed, ii) the person holds the material and iii) the material requested will be of substantial value to the investigation and iv) it is in the public interest that the material should be produced.

⁴ All references to the Police and Criminal Evidence Act 1984 shall be interpreted, insofar as the Code relates to activity in Northern Ireland, as referring to the Police and Criminal Evidence (Northern Ireland) Order 1989.

⁵ Or a County court judge in Northern Ireland.

4. Special rules on interception with a warrant

Collateral intrusion

- 4.1 Consideration should be given to any interference with the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament⁶ and another person on constituency business may be involved or communications between a Member of Parliament and a whistle-blower. An application for an interception warrant should state whether the interception is likely to give rise to a degree of collateral infringement of privacy. A person applying for an interception warrant must also consider measures, including the use of automated systems, to reduce the extent of collateral intrusion. Where it is possible to do so, the application should specify those measures. These circumstances and measures will be taken into account by the Secretary of State when considering a warrant application made under section 8(1) of RIPA. Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right, consideration should be given to applying for separate warrants covering those individuals.

Confidential information

- 4.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the communications relate to legally privileged material; where confidential journalistic material may be involved; where interception might involve communications between a medical professional or Minister of Religion and an individual relating to the latter's health or spiritual welfare; or where communications between a Member of Parliament and another person on constituency business may be involved.
- 4.3 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. See also paragraphs 4.26 and 4.28 - 4.31 for additional safeguards that should be applied in respect of confidential journalistic material.
- 4.4 The Prime Minister must be consulted in any case where it is necessary to target the communications of a Member of Parliament, apart from those approved by Scottish Ministers, or where it is intended to select for examination an MP's communications intercepted under a section 8(4) warrant.

⁶ References to a Member of Parliament include references to a member of the House of Commons, the House of Lords, a UK member of the European Parliament, and members of the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly.

Communications subject to legal privilege

Introduction

- 4.5 Section 98 of the Police Act 1997 describes those matters that are subject to legal privilege in England and Wales. In Scotland, those matters subject to legal privilege contained in section 412 of the Proceeds of Crime Act 2002 should be adopted. With regard to Northern Ireland, Article 12 of the Police and Criminal Evidence (Northern Ireland) Order 1989 should be referred to.
- 4.6 Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications will lose their protection if, for example, the professional legal adviser is intending to hold or use the information for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.
- 4.7 For the purposes of this Code, any communication between lawyer and client, or between a lawyer and another person for the purpose of actual or contemplated litigation (whether civil or criminal), must be presumed to be privileged unless the contrary is established: for example, where it is plain that the communication does not form part of a professional consultation of the lawyer, or there is clear and compelling evidence that the 'furthering a criminal purpose' exemption applies. Where there is doubt as to whether the communications are subject to legal privilege or over whether communications are not subject to legal privilege due to the "in furtherance of a criminal purpose" exception, advice should be sought from a legal adviser within the relevant intercepting agency.
- 4.8 RIPA does not provide any special protection for legally privileged communications. Nevertheless, intercepting such communications (or selecting them for examination in accordance with section 16 when intercepted under a section 8(4) warrant) is particularly sensitive and may give rise to issues under Article 6 (right to a fair trial) of the ECHR as well as engaging Article 8. The interception of communications subject to legal privilege (whether deliberately obtained or otherwise) is therefore subject to additional safeguards under this code as set out at paragraphs 4.9-4.15 below. The guidance set out below may in part depend on whether matters subject to legal privilege have been obtained intentionally or incidentally to other material which has been sought.

Application process for section 8(1) warrants

- 4.9 Where interception under a section 8(1) warrant is likely to result in a person acquiring communications subject to legal privilege, the application should include, in addition to the reasons why it is considered necessary for the interception to take place, an assessment of how likely it is that communications which are subject to legal privilege will be intercepted. In addition, it should state whether the purpose (or one of the purposes) of the interception is to obtain privileged communications. Where the intention is not to acquire communications subject to legal privilege, but it is likely that such communications will nevertheless be acquired during interception, that should be made clear in the warrant application and the relevant agency should confirm that any inadvertently obtained communications that are subject to legal privilege will be treated in accordance with the

safeguards set out in this chapter and that reasonable and appropriate steps will be taken to minimise access to the communications subject to legal privilege.

- 4.10 Where the intention is to acquire legally privileged communications, the Secretary of State will only issue the warrant under section 8(1) if satisfied that there are exceptional and compelling circumstances that make the authorisation necessary. Such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb or to national security, and the interception is reasonably regarded as likely to yield intelligence necessary to counter the threat.
- 4.11 Further, in considering any such application, the Secretary of State must believe that the proposed conduct is proportionate to what is sought to be achieved. In particular the Secretary of State must consider whether the purpose of the proposed interception could be served by obtaining non-privileged information. In such circumstances, the Secretary of State will be able to impose additional conditions such as regular reporting arrangements, so as to be able to exercise his or her discretion on whether a warrant should continue to have effect.
- 4.12 Where there is a renewal application in respect of a warrant which has resulted in the obtaining of legally privileged material, that fact should be highlighted in the renewal application.

Selection for examination of legally privileged section 8(4) material: requirement for prior approval by independent senior official

- 4.13 Where material intercepted under section 8(4) is to be selected for examination according to a factor that is intended, or is likely to, result in a person acquiring communications subject to legal privilege, the enhanced procedure described at paragraph 4.14 and 4.15 applies.
- 4.14 An authorised person in a public authority must notify a senior official⁸ before using a factor to select any section 8(4) material for examination, where this will, or is likely to, result in the acquisition of legally privileged communications. The notification must address the same considerations as described in paragraph 4.9. The senior official, who must not be a member of the public authority to whom the section 8(4) warrant is addressed, must in any case where the intention is to acquire communications subject to legal privilege, apply the same tests and considerations as described in paragraph 4.10 and 4.11. The authorised person is prohibited from accessing the material until he or she has received approval from the senior official authorising the selection of communications subject to legal privilege.
- 4.15 In the event that privileged communications are inadvertently and unexpectedly selected for examination (and where the enhanced procedure in paragraph 4.14 has consequently not been followed), any material so obtained must be handled strictly in accordance with the provisions of this chapter. No further privileged communications may be selected for examination by reference to that factor unless approved by the senior official as set out in paragraph 4.14.

⁷ See chapter 6.

⁸ Senior official is defined in section 81 of RIPA.

Lawyers' communications

- 4.16 Where a lawyer is the subject of an interception under a section 8(1) warrant or selected for examination in accordance with section 16, it is possible that a substantial proportion of the communications which will be intercepted or selected will be between the lawyer and his or her client(s) and will be subject to legal privilege. Therefore, and for the avoidance of doubt, in any case where a lawyer is the subject of an interception or selection for examination, the application or notification must be made on the basis that it is intended to acquire communications subject to legal privilege and the provisions in paragraphs 4.10, 4.11 and 4.14 will apply, as relevant.
- 4.17 Any case where a lawyer is the subject of an interception or whose communications have been selected for examination in accordance with section 16 should also be notified to the Interception of Communications Commissioner during his or her next inspection and any material which has been retained should be made available to the Commissioner on request.

Handling, retention and deletion

- 4.18 In addition to safeguards governing the handling and retention of intercept material as provided for in section 15 of RIPA, officials who examine intercepted communications should be alert to any intercept material which may be subject to legal privilege.
- 4.19 Where it is discovered that privileged material has been obtained inadvertently, an early assessment must be made of whether it is necessary and proportionate to retain it for one or more of the authorised purposes set out in section 15(4). If not, the material should be securely destroyed as soon as possible.
- 4.20 Material which has been identified as legally privileged should be clearly marked as subject to legal privilege. Such material should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 15(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such material is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

Dissemination

- 4.21 Material subject to legal privilege must not be acted on or further disseminated unless a legal adviser has been consulted on the lawfulness (including the necessity and proportionality) of such action or dissemination.
- 4.22 The dissemination of legally privileged material to an outside body should be accompanied by a clear warning that it is subject to legal privilege. It should be safeguarded by taking reasonable steps to remove the risk of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings to which the information relates, including law enforcement authorities. In this regard civil proceedings includes all legal proceedings before courts and tribunals that are not criminal in nature. Neither the Crown Prosecution Service lawyer nor any other prosecuting authority lawyer with conduct of a prosecution should have sight of any communications subject to legal privilege, held by the relevant public authority, with any possible connection to the proceedings. In respect of civil

proceedings, there can be no circumstances under which it is proper for any public authority to have sight of or seek to rely on communications subject to legal privilege in order to gain a litigation advantage over another party in legal proceedings.

- 4.23 In order to safeguard against any risk of prejudice or accusation of abuse of process, public authorities must also take all reasonable steps to ensure that (so far as practicable) lawyers or policy officials with conduct of legal proceedings should not see legally privileged communications relating to those proceedings (whether the privilege is that of the other party to those proceedings or that of a third party). If such circumstances do arise, the public authority must seek independent advice from Counsel and, if there is assessed to be a risk that sight of such material could yield a litigation advantage, the direction of the Court must be sought.

Reporting to the Commissioner

- 4.24 In those cases where communications which include legally privileged communications have been intercepted and retained, the matter should be reported to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material that is still being retained should be made available to him or her if requested, including detail of whether that material has been disseminated.
- 4.25 For the avoidance of doubt, the guidance in paragraphs 4.7 to 4.24 takes precedence over any contrary content of an agency's internal advice or guidance.

Communications involving confidential journalistic material, confidential personal information and communications between a Member of Parliament and another person on constituency business

- 4.26 Particular consideration must also be given to the interception of communications that involve confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business. Confidential journalistic material is explained at paragraph 4.3. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.
- 4.27 Spiritual counselling is defined as conversations between an individual and a Minister of Religion acting in his or her official capacity, and where the individual being counselled is seeking, or the Minister is imparting, forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.
- 4.28 Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not

intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the intercepting agency.

- 4.29 Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 15(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.
- 4.30 Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material takes place.
- 4.31 Any case where confidential information is retained should be notified to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material which has been retained should be made available to the Commissioner on request.
- 4.32 The safeguards set out in paragraphs 4.28 – 4.31 also apply to any section 8(4) material (see chapter 6) which is selected for examination and which constitutes confidential information.

archived

5. Interception warrants (section 8(1))

- 5.1 This section applies to the interception of communications by means of a warrant complying with section 8(1) of RIPA. This type of warrant may be issued in respect of the interception of communications carried on any postal service or telecommunications system as defined in section 2(1) of RIPA (including a private telecommunications system). Responsibility for the issuing of interception warrants rests with the Secretary of State.

Application for a section 8(1) warrant

- 5.2 An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. A copy may then be served on any person who may be able to provide assistance in giving effect to that warrant. Prior to submission to the Secretary of State, each application should be subject to a review within the agency seeking the warrant. This review involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of RIPA and whether the interception proposed is both necessary and proportionate. Each application, a copy of which should be retained by the intercepting agency, should contain the following information:
- Background to the operation in question;
 - Person or premises to which the application relates (and how the person or premises feature in the operation);
 - Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the interception operation where this is relevant;⁹
 - Description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.¹⁰ This conduct may include the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a);
 - An explanation of why the interception is considered to be necessary under the provisions of section 5(3);
 - Consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
 - Consideration of any collateral intrusion and why that intrusion is justified in the circumstances;
 - Whether the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, or communications between a Member of Parliament and another person on constituency business;

⁹ This assessment is normally based upon information provided by the relevant communications service provider.

¹⁰ Section 20 of the Act defines related communications data as being that data (within the meaning of Part I Chapter II of the Act) as is obtained by, or in connection with, the interception (under warrant); and relates to the communication to the sender or recipient, or intended recipient of the communication.

- Where an application is urgent, the supporting justification;
- An assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of RIPA (see paragraph 7.2).

Authorisation of a section 8(1) warrant

5.3 Before issuing a warrant under section 8(1), the Secretary of State must believe the warrant is necessary:¹¹

- In the interests of national security;
- For the purpose of preventing or detecting serious crime; or
- For the purpose of safeguarding the economic well-being of the UK, so far as those interests are also relevant to the interests of national security.

5.4 The Secretary of State will not issue a warrant on section 5(3)(c) grounds if this direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore explain how, in the applicant's view, the economic well-being of the UK which is to be safeguarded is directly related to national security on the facts of the case.

5.5 The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

Urgent authorisation of a section 8(1) warrant

5.6 RIPA makes provision (section 7(4)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. RIPA restricts issuing warrants in this way to urgent cases where the Secretary of State has expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)). A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed by the Secretary of State. If it is renewed it expires after three months in the case of serious crime, or six months in the case of national security or economic well-being, in the same way as other non-urgent section 8(1) warrants.

Format of a section 8(1) warrant

5.7 Each warrant comprises two sections: a warrant instrument signed by the Secretary of State listing the subject of the interception or set of premises - a copy of which each CSP will receive - and a schedule or set of schedules listing the communications to be intercepted. Only the schedule relevant to the communications that can be intercepted by the specified CSP may be provided to that CSP.

¹¹ A single warrant can be justified on more than one of the grounds listed.

5.8 The warrant instrument should include:

- The name or description of the interception subject or of a set of premises in relation to which the interception is to take place;
- A warrant reference number; and
- The persons who may subsequently modify the scheduled part of the warrant in an urgent case (if authorised in accordance with section 10(8) of RIPA).

5.9 The scheduled part of the warrant will comprise one or more schedules. Each schedule should contain:

- The name of the communication service provider, or the other person who is to take action;
- A warrant reference number; and
- A means of identifying the communications to be intercepted.¹²

Modification of a section 8(1) warrant

5.10 Interception warrants may be modified under the provisions of section 10 of RIPA. The unscheduled part of a warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases, a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is renewed by the Secretary of State. The modification will then expire upon the expiry date of the warrant.

5.11 Scheduled parts of a warrant may be modified by the Secretary of State, or by a senior official¹³ acting upon his or her behalf. A modification to the scheduled part of the warrant may include the addition of a new schedule relating to a CSP on whom a copy of the warrant has not been previously served. Modifications made in this way expire at the same time as the warrant expires. There also exists a duty to modify a warrant by deleting a communication identifier if it is no longer relevant. When a modification is sought to delete a number or other communication identifier, the relevant CSP must be advised and interception suspended before the modification instrument is signed.

5.12 The person to whom the warrant is addressed or a senior official within the same agency may modify the scheduled part of the warrant if the warrant was issued or renewed on national security grounds.¹⁴ Where the warrant specifically authorises it, the scheduled part of the warrant may also be amended in an urgent case by the person to whom the warrant is addressed or a subordinate person (identified in the warrant) within the same agency.¹⁵

¹² This may include addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying communications (section 8(2) of RIPA).

¹³ The official to whom the warrant is addressed, or any of his subordinates, may only modify the scheduled parts of the warrant in the circumstances referred to in paragraph 5.12.

¹⁴ Under section 10(6) and (6A) RIPA.

¹⁵ Under section 10(8) RIPA.

- 5.13 Modifications of this kind are valid for five working days following the date of issue unless the modification instrument is endorsed within that period by a senior official acting on behalf of the Secretary of State. Where the modification is endorsed in this way, the modification expires upon the expiry date of the warrant.

Renewal of a section 8(1) warrant

- 5.14 The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals must be made to the Secretary of State and should contain an update of the matters outlined in paragraph 5.2 above. In particular, the applicant should give an assessment of the value of interception to the operation to date and explain why it is considered that interception continues to be necessary for one or more of the purposes in section 5(3), and why it is considered that interception continues to be proportionate.
- 5.15 Where the Secretary of State is satisfied that the interception continues to meet the requirements of RIPA the Secretary of State may renew the warrant.
- 5.16 A copy of the warrant renewal instrument will be forwarded to all relevant CSPs on whom a copy of the original warrant instrument and a schedule have been served, providing they are still actively assisting. A warrant renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

- 5.17 The Secretary of State is under a duty to cancel an interception warrant if, at any time before its expiry date, the Secretary of State is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.
- 5.18 The cancellation instrument should be addressed to the person to whom the warrant was issued (the intercepting agency) and should include the reference number of the warrant and the description of the person or premises specified in the warrant. A copy of the cancellation instrument should be sent to those CSPs who have held a copy of the warrant instrument and accompanying schedule during the preceding twelve months.

Records

- 5.19 The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State's decision was based, and the applicant may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:
- All applications made for warrants complying with section 8(1) and applications made for the renewal of such warrants;
 - All warrants, and renewals and copies of schedule modifications (if any);

- Where any application is refused, the grounds for refusal as given by the Secretary of State; and
 - The dates on which interception started and stopped.
- 5.20 Records should also be kept of the arrangements by which the requirements of section 15(2) (minimisation of copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see the section on "Safeguards".
- 5.21 The term 'intercepted material' is used throughout to include any copy, extract or summary made from the intercepted material which identifies itself as the product of an interception as well as the intercepted material itself.

archived

6. Interception warrants (section 8(4))

- 6.1 This section applies to the interception of external communications by means of a warrant complying with section 8(4) of RIPA.
- 6.2 In contrast to section 8(1), a section 8(4) warrant instrument need not name or describe the interception subject or a set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted. For example, if the requirements of sections 8(4) and (5) are met, then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified.
- 6.3 Responsibility for the issuing of interception warrants under section 8(4) of RIPA rests with the Secretary of State. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate. The certificate ensures that a selection process is applied to the intercepted material so that only material described in the certificate is made available for human examination. If the intercepted material cannot be selected to be read, looked at or listened to with due regard to proportionality and the terms of the certificate, then it cannot be read, looked at or listened to by anyone.

Section 8(4) interception in practice

- 6.4 A section 8(4) warrant authorises the interception of external communications. Where a section 8(4) warrant results in the acquisition of large volumes of communications, the intercepting agency will ordinarily apply a filtering process to automatically discard communications that are unlikely to be of intelligence value. Authorised persons within the intercepting agency may then apply search criteria to select communications that are likely to be of intelligence value in accordance with the terms of the Secretary of State's certificate. Before a particular communication may be accessed by an authorised person within the intercepting agency, the person must provide an explanation of why it is necessary for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State, and why it is proportionate in the particular circumstances. This process is subject to internal audit and external oversight by the Interception of Communications Commissioner. Where the Secretary of State is satisfied that it is necessary, he or she may authorise the selection of communications of an individual who is known to be in the British Islands. In the absence of such an authorisation, an authorised person must not select such communications.¹⁶

¹⁶ Section 16(2) of RIPA provides that in the absence of such an authorisation an authorised person must not select communications for examination by factors referable to an individual known to be in the British Islands and with the purpose of identifying material contained in communications sent by or intended for such an individual.

Definition of external communications

- 6.5 External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.

Intercepting non-external communications under section 8(4) warrants

- 6.6 Section 5(6)(a) of RIPA makes clear that the conduct authorised by a section 8(4) warrant may, in principle, include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates.
- 6.7 When conducting interception under a section 8(4) warrant, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State under section 8(4). It must also conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the objective of intercepting wanted external communications.

Application for a section 8(4) warrant

- 6.8 An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC)¹⁷.
- 6.9 Prior to submission, each application is subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of RIPA and whether the interception proposed is both necessary and proportionate.
- 6.10 Each application, a copy of which must be retained by the applicant, should contain the following information:
- Background to the operation in question:
 - Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where this is relevant;¹⁸ and

¹⁷ One of the NSC's functions is to set the priorities for intelligence coverage for GCHQ and SIS.

¹⁸ This assessment is normally based upon information provided by the relevant communications service provider.

- o Description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of RIPA) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.
- The certificate that will regulate examination of intercepted material;
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Where an application is urgent, supporting justification;
- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of sections 16(2)-16(6) of RIPA; and
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA (see paragraphs 7.2 and 7.10 respectively).

Authorisation of a section 8(4) warrant

- 6.11 Before issuing a warrant under section 8(4), the Secretary of State must believe the warrant is necessary:
- In the interests of national security;
 - For the purpose of preventing or detecting serious crime; or
 - For the purpose of safeguarding the economic well-being of the UK so far as those interests are also relevant to the interests of national security.
- 6.12 The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK (as provided for by section 5(3)(c) of RIPA), may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore identify the circumstances that are relevant to the interests of national security.
- 6.13 The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).
- 6.14 When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he or she considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. The purpose of the statutory certificate is to ensure that a selection process is applied to intercepted material so that only material described in the certificate is made available for human examination. Any certificate must broadly reflect the "Priorities for Intelligence

Collection* set by the NSC for the guidance of the intelligence agencies. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971). The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.

- 6.15 The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 16(2) to section 16(6) is, in fact, read, looked at or listened to. The Interception of Communications Commissioner is under a duty to review the adequacy of those arrangements.

Urgent authorisation of a section 8(4) warrant

- 6.16 RIPA makes provision (section 7(1)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. RIPA restricts the issue of warrants in this way to urgent cases where the Secretary of State has personally and expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)).
- 6.17 A warrant issued under the urgency procedure lasts for five working days following the date of issue unless renewed by the Secretary of State, in which case it expires after three months in the case of serious crime or six months in the case of national security or economic well-being, in the same way as other section 8(4) warrants.

Format of a section 8(4) warrant

- 6.18 Each warrant is addressed to the person who submitted the application. A copy may then be served upon such providers of communications services as he or she believes will be able to assist in implementing the interception. CSPs will not normally receive a copy of the certificate. The warrant should include the following:
- A description of the communications to be intercepted;
 - The warrant reference number; and
 - Details of the persons who may subsequently modify the certificate applicable to the warrant in an urgent case (if authorised in accordance with section 10(7) of RIPA).

Modification of a section 8(4) warrant and/or certificate

- 6.19 Interception warrants and certificates may be modified under the provisions of section 10 of RIPA. A warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

- 6.20 A certificate must be modified by the Secretary of State, except in an urgent case where a certificate may be modified by a senior official provided that the official holds a position in which he or she is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf, or the Secretary of State has expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument. In the latter case, the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.
- 6.21 Where the Secretary of State is satisfied that it is necessary, a certificate may be modified to authorise the selection of communications of an individual in the British Islands.¹⁹ An individual's location should be assessed using all available information. If it is not possible, to determine definitively where the individual is located using that information, an informed assessment should be made, in good faith, as to the individual's location. If an individual is strongly suspected to be in the UK, the arrangements set out in this paragraph will apply.

Renewal of a section 8(4) warrant

- 6.22 The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 6.19 above. In particular, the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the purposes in section 5(3), and why it is considered that interception continues to be proportionate.
- 6.23 Where the Secretary of State is satisfied that the interception continues to meet the requirements of RIPA, the Secretary of State may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/ economic well-being grounds the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.
- 6.24 In those circumstances where the assistance of CSPs has been sought, a copy of the warrant renewal instrument will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

Warrant cancellation

- 6.25 The Secretary of State must cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a

¹⁹ Section 16(3) of RIPA provides that a certificate may be modified to authorise the selection of communications sent or received outside the British Islands according to a factor (for example name, email address or passport number) which is referable to an individual who is known for the time being to be in the British Islands and where the purpose is the identification of material contained in communications sent by that individual or intended for him.

warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

- 6.26 The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those CSPs, if any, who have given effect to the warrant during the preceding twelve months.

Records

- 6.27 The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State's decision is based, and the interception agency may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:
- All applications made for warrants complying with section 8(4), and applications made for the renewal of such warrants;
 - All warrants and certificates, and copies of renewal and modification instruments (if any);
 - Where any application is refused, the grounds for refusal as given by the Secretary of State;
 - The dates on which interception started and stopped.
- 6.28 Records should also be kept of the arrangements for securing that only material which has been certified for examination for a purpose under section 5(3) and which meets the conditions set out in section 16(2) – 16(6) of RIPA in accordance with section 15 of RIPA is, in fact, read, looked at or listened to. Records should be kept of the arrangements by which the requirements of section 15(2) (minimisation of copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see the chapter on "Safeguards".

7. Safeguards

- 7.1 All material intercepted under the authority of a warrant complying with section 8(1) or section 8(4) of RIPA and any related communications data²⁰ must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed on him or her by RIPA. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of RIPA which are set out below. In addition, the safeguards in section 16 of RIPA apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner. The intercepting agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

The section 15 safeguards

- 7.2 Section 15 of RIPA requires that disclosure, copying and retention of intercepted material is limited to the minimum necessary for the authorised purposes. Section 15(4) of RIPA provides that something is necessary for the authorised purposes if the intercepted material:
- Continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK²¹;
 - Is necessary for facilitating the carrying out of the functions of the Secretary of State under Chapter I of Part I of RIPA;
 - Is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal;
 - Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or
 - Is necessary for the performance of any duty imposed by the Public Record Acts.

²⁰ References in this code to 'intercepted material' include for the purposes of section 15 any related communications data. Further information regarding the use of related communications data is to be found in the Acquisition and Disclosure of Communications Data Code of Practice.

²¹ Intercepted material and related communications data obtained for one purpose can, where it is necessary and proportionate to do so, be disclosed, copied and retained for another.

Dissemination of intercepted material

- 7.3 The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted material may be disclosed as the recipient needs. For example, if a summary of the intercepted material will suffice, no more than that should be disclosed.
- 7.4 The obligations apply not just to the original interceptor, but also to anyone to whom the intercepted material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the intercepted material further. In others, explicit safeguards are applied to secondary recipients.
- 7.5 Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. In particular, the intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

Copying

- 7.6 Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 15(4) of RIPA. Copies include not only direct copies of the whole of the intercepted material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which includes the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

Storage

- 7.7 Intercepted material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This requirement to store intercept product securely applies to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with the Government before a Section 12 Notice is served (see paragraph 3.13).

Destruction

- 7.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be marked for deletion and securely destroyed as soon as possible once it is no longer needed for any of the authorised purposes. If such intercepted material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of RIPA.
- 7.9 Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

Personnel security

- 7.10 All persons who may have access to intercepted material or need to see any reporting in relation to it must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one agency to disclose intercepted material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

The section 16 safeguards

- 7.11 Section 16 provides for additional safeguards in relation to intercepted material gathered under section 8(4) warrants, requiring that the safeguards:
- Ensure that intercepted material is read, looked at or listened to by any person only to the extent that the intercepted material is certified; and
 - Regulate the use of selection factors that refer to the communications of individuals known to be currently in the British Islands.
- 7.12 In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given section 6(1) of the Human Rights Act 1998).
- 7.13 The certificate ensures that a selection process is applied to material intercepted under section 8(4) warrants so that only material described in the certificate is made available for human examination (in the sense of being read, looked at or listened to). No official is permitted to gain access to the data other than as permitted by the certificate.

- 7.14 In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 16(1) of RIPA. As an exception, a certificate may permit intercepted material to be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the certificate, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in section 5(3) of RIPA. Once those functions have been fulfilled, any copies made of the material for those purposes must be destroyed in accordance with section 15(3) of RIPA. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Interception of Communications Commissioner during his or her inspections.
- 7.15 Material gathered under a section 8(4) warrant should be read, looked at or listened to only by authorised persons who receive regular mandatory training regarding the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory safeguards. All authorised persons must be appropriately vetted (see paragraph 7.10 for further information).
- 7.16 Prior to an authorised person being able to read, look at or listen to material, a record²² should be created setting out why access to the material is required consistent with, and pursuant to, section 16 and the applicable certificate, and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 7.14, the record must indicate, by reference to specific factors, the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. The record should include any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of the collateral intrusion. All records must be retained for the purposes of subsequent examination or audit.
- 7.17 Access to the material as described in paragraph 7.15 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted. When access to the material is no longer sought, the reason for this must also be explained in the record.
- 7.18 Periodic audits should be carried out to ensure that the requirements set out in section 16 of RIPA and Chapter 3 of this code are being met. These audits must include checks to ensure that the records requesting access to material to be read, looked at, or listened to have been correctly compiled, and specifically, that the material requested falls within matters certified by the Secretary of State. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards (as noted in paragraph 7.1) must be reported to the Interception of

²² Any such record should be made available to the Commissioner on request for purposes of oversight.

Communications Commissioner. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

- 7.19 In order to meet the requirements of RIPA described in paragraph 6.3 above, where a selection factor refers to an individual known to be for the time being in the British Islands, and has as its purpose or one of its purposes, the identification of material contained in communications sent by or intended for him or her, a submission must be made to the Secretary of State, or to a senior official in an urgent case, giving an explanation of why an amendment to the section 8(4) certificate in relation to such an individual is necessary for a purpose falling within section 5(3) of RIPA and is proportionate in relation to any conduct authorised under section 8(4) of RIPA.
- 7.20 The Secretary of State must ensure that the safeguards are in force before any interception under section 8(4) warrants can begin. The Interception of Communications Commissioner is under a duty to review the adequacy of the safeguards.

archived

8. Disclosure to ensure fairness in criminal proceedings

- 8.1 Section 15(3) of RIPA contains the general rule that intercepted material must be destroyed as soon as its retention is no longer necessary for a purpose authorised under RIPA. Section 15(4) specifies the authorised purposes for which retention is necessary.
- 8.2 This part of the code applies to the handling of intercepted material in the context of criminal proceedings where the material has been retained for one of the purposes authorised in section 15(4) of RIPA. For those who would ordinarily have had responsibility under the Criminal Procedure and Investigations Act 1996 to provide disclosure in criminal proceedings, this includes those rare situations where destruction of intercepted material has not taken place in accordance with section 15(3) and where that material is still in existence after the commencement of a criminal prosecution. In these circumstances, retention will have been considered necessary to ensure that a person conducting a criminal prosecution has the information he or she needs to discharge his or her duty of ensuring its fairness (section 15(4)(d)).

Exclusion of matters from legal proceedings

- 8.3 The general rule is that neither the possibility of interception, nor intercepted material itself, plays any part in legal proceedings. This rule is set out in section 17 of RIPA, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Act (or the Interception of Communications Act 1985). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves "equality of arms" which is a requirement under Article 6 of the ECHR.
- 8.4 Section 18 contains a number of tightly-drawn exceptions to this rule. This part of the code deals only with the exception in subsections (7) to (11).

Disclosure to a prosecutor

- 8.5 Section 18(7)(a) provides that intercepted material obtained by means of a warrant and which continues to be available may, for a strictly limited purpose, be disclosed to a person conducting a criminal prosecution.
- 8.6 This may only be done for the purpose of enabling the prosecutor to determine what is required of him or her by his or her duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he or she is given access under section 18(7)(a) to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings.
- 8.7 The exception does not mean that intercepted material should be retained against a remote possibility that it might be relevant to future proceedings. The normal expectation is still for the intercepted material to be destroyed in accordance with the general safeguards provided by section 15. The exceptions only come into play if such material

has, in fact, been retained for an authorised purpose. Because the authorised purpose given in section 5(3)(b) ("*for the purpose of preventing or detecting serious crime*") does not extend to gathering evidence for the purpose of a prosecution, material intercepted for this purpose may not have survived to the prosecution stage, as it will have been destroyed in accordance with the section 15(3) safeguards. There is, in these circumstances, no need to consider disclosure to a prosecutor if, in fact, no intercepted material remains in existence.

- 8.8 Section 18(7)(a) recognises the duty on prosecutors, acknowledged by common law, to review all available material to make sure that the prosecution is not proceeding unfairly. 'Available material' will only ever include intercepted material at this stage if the conscious decision has been made to retain it for an authorised purpose.
- 8.9 If intercepted material does continue to be available at the prosecution stage, once this information has come to the attention of its holder, the prosecutor should be informed that a warrant has been issued under section 5 and that material of possible relevance to the case has been intercepted.
- 8.10 Having had access to the material, the prosecutor may conclude that the material affects the fairness of the proceedings. In these circumstances, he or she will decide how the prosecution, if it proceeds, should be presented.

Disclosure to a judge

- 8.11 Section 18(7)(b) recognises that there may be cases where the prosecutor, having seen intercepted material under subsection (7)(a), will need to consult the trial judge. Accordingly, it provides for the judge to be given access to intercepted material, where there are exceptional circumstances making that disclosure essential in the interests of justice.
- 8.12 This access will be achieved by the prosecutor inviting the judge to make an order for disclosure to him or her alone, under this subsection. This is an exceptional procedure; normally, the prosecutor's functions under subsection (7)(a) will not fall to be reviewed by the judge. To comply with section 17(1), any consideration given to, or exercise of, this power must be carried out without notice to the defence. The purpose of this power is to ensure that the trial is conducted fairly.
- 8.13 The judge may, having considered the intercepted material disclosed to him or her, direct the prosecution to make an admission of fact. The admission will be abstracted from the interception, but, in accordance with the requirements of section 17(1), it must not reveal the fact of interception. This is likely to be a very unusual step. RIPA only allows it where the judge considers it essential in the interests of justice.
- 8.14 Nothing in these provisions allows intercepted material, or the fact of interception, to be disclosed to the defence.

9. Interception without a warrant

- 9.1 Lawful interception can only take place if the conduct has lawful authority (as set out in section 1(5) of RIPA). Section 1(5) of RIPA permits interception without a warrant in the following circumstances:
- Where it is authorised by or under sections 3 or 4 of RIPA (see below), or
 - Where it takes place, in relation to any stored communication, under some other statutory power being exercised for the purpose of obtaining information or of taking possession of any document or other property. This includes, for example, the obtaining of a production order under Schedule 1 to the Police and Criminal Evidence Act 1984 for stored communications to be produced.
- 9.2 Interception in accordance with a warrant under section 5 of RIPA is dealt with under chapters 3, 4, 5 and 6 of this code. Interception without lawful authority may be a criminal offence (see paragraph 2.2 of this code).
- 9.3 There is no prohibition in RIPA on the evidential use of any material that is obtained as a result of lawful interception which takes place without a warrant, pursuant to sections 3 or 4 of RIPA, or pursuant to some other statutory power. The matter may still, however, be regulated by the exclusionary rules of evidence to be found in the common law, section 78 of the Police and Criminal Evidence Act 1984, and/or pursuant to the Human Rights Act 1998.

Interception with the consent of both parties

- 9.4 Section 3(1) of RIPA authorises the interception of a communication if both the person sending the communication and the intended recipient(s) have given their consent.

Interception with the consent of one party

- 9.5 Section 3(2) of RIPA authorises the interception of a communication if either the sender or intended recipient of the communication has consented to its interception, and directed surveillance by means of that interception has been authorised under Part II of RIPA or authorised under The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). Further details can be found in chapter 2 of the Covert Surveillance and Property Interference Code of Practice and in chapter 3 of the Covert Human Intelligence Sources Code of Practice²³, or their RIPSA equivalents.

Interception for the purposes of a communication service provider

- 9.6 Section 3(3) of RIPA permits a communication service provider, or a person acting upon their behalf, to carry out interception for purposes connected with the operation of that service, or for purposes connected with the enforcement of any enactment relating to the use of the communication service.

²³ <http://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>

Lawful business practice

- 9.7 Section 4(2) of RIPA enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept communications for the purpose of carrying on a business. These regulations apply equally to public authorities. These Lawful Business Practice Regulations can be found on the [legislation.gov.uk](http://www.legislation.gov.uk) website:

<http://www.legislation.gov.uk/uksi/2000/2699>

archived

10. Oversight

- 10.1 RIPA provides for an Interception of Communications Commissioner, whose remit is to provide independent oversight of the use of the powers contained within the warranted interception regime under Chapter I of Part I of RIPA.
- 10.2 The Commissioner carries out biannual inspections of each of the nine interception agencies. The primary objectives of the inspections are to ensure that the Commissioner has the information he or she requires to carry out his or her functions under section 57 of RIPA and produce his or her report under section 58 of RIPA. This may include inspection or consideration of:
- The systems in place for the interception of communications;
 - The relevant records kept by the intercepting agency;
 - The lawfulness of the interception carried out; and
 - Any errors and the systems designed to prevent such errors.
- 10.3 Any person who exercises the powers in RIPA Part I Chapter I must report to the Commissioner any action that is believed to be contrary to the provisions of RIPA or any inadequate discharge of section 15 safeguards. He or she must also comply with any request made by the Commissioner to provide any such information as the Commissioner requires for the purpose of enabling him or her to discharge his or her functions.

11. Complaints

- 11.1 RIPA establishes an independent tribunal, the Investigatory Powers Tribunal. The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and determine complaints against public authority use of covert powers and human rights claims against the intelligence agencies. It may decide any case within its jurisdiction.
- 11.2 This code does not cover the exercise of the Tribunal's functions. Details of the relevant complaints procedure are available on the IPT website at: <http://www.ipt-uk.com> or can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ
0207 035 3711

archived

12. Rules for requesting and handling unanalysed intercepted communications from a foreign government

Application of this chapter

- 12.1 This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.

Requests for assistance other than in accordance with an international mutual assistance agreement

- 12.2 A request may only be made by an intercepting agency to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual assistance agreement, if either:
- A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or
 - Making the request for the particular communications in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications.
- 12.3 A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.
- 12.4 For these purposes, a "relevant RIPA interception warrant" means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications (for other individuals).

Safeguards applicable to the handling of unanalysed intercepted communications from a foreign government

- 12.5 If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors.²⁴
- 12.6 Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content²⁵ and communications data²⁶ must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.
- 12.7 All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner.

²⁴ All other requests within paragraph 12.2 (whether with or without a relevant RIPA interception warrant) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s) as set out in paragraphs 12.2.

²⁵ Whether analysed or unanalysed.

²⁶ Whether or not those data are associated with the content of communications.

archived

This document was withdrawn on 5 April 2016.

archived

archived

This document was withdrawn on 5 April 2016.

archived

This document was withdrawn on 5 April 2016.

archived

ISBN 978-1-4741-2475-1



9 781474 124751

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/14/85/CH

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/120-126/CH

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

1. I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also have wider responsibilities for GCHQ's external communications and policy. I have been in this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

1 of 23

2. I am authorised to make this witness statement on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.
3. Attached to this statement and marked Exhibit ['CM1'] is a bundle of relevant documents. Tab and page numbers below are references to that Exhibit.
4. In this statement I use the term "the intelligence services" to refer, collectively, to the Security Service, the Secret Intelligence Service and the Government Communications Headquarters. I also use the terms "MI5", "SIS" and "GCHQ" to refer to those bodies individually.
5. In this statement I will (I) address the current intelligence picture and the ongoing challenges posed by changes in technology and developments in the communications market, (II) provide an overview of Computer and Network Exploitation (CNE) and its importance and value in fulfilling GCHQ's statutory functions, before (III) addressing some key safeguards and oversight mechanisms for CNE activities carried out by GCHQ, including:
 - a) The processes for applying for warrants under section 5 of the Intelligence Services Act 1994;
 - b) The processes for applying for section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals;
 - c) Oversight by the Intelligence Services Commissioner, a retired senior judge;
 - d) Oversight by the Intelligence and Security Committee of Parliament (ISC).

I. THE CURRENT INTELLIGENCE PICTURE

6. The intelligence background to the preliminary issues of law in the *Liberty/Privacy* proceedings was set out in paragraphs 8 to 19 of the witness statement dated 16th May 2014 of Charles Farr, Director General of the Office for Security and Counter Terrorism (OSCT) at the Home Office. I adopt and agree with that statement of the background as it then stood. Given the passage of time, it is necessary to update it and I do so below.
7. Over the past year, the threat to the UK from international terrorism in particular has continued to increase. On the 17 September 2015, Andrew Parker, the Director General of the Security Service (MI5), during an interview with the BBC, revealed that six alleged terror plots targeting the UK have been stopped in the preceding twelve months during an interview with the BBC. In August 2014, the UK threat level, assessed independently by the Joint Terrorism Analysis Centre ("JTAC"), was raised to "SEVERE" from "SUBSTANTIAL", which means that an attack in the UK is highly likely. The principal terrorist threat to the UK continues to derive from militant Islamist terrorists, particularly in Syria and Iraq, where the Islamic State of Iraq and the Levant ("ISIL") has emerged as the most violent of the terrorist groups operating in that region.

8. The recent 2014 Annual Report by the Home Office on the UK's Counter-Terrorism Strategy ("the CONTEST Report"), published on 23 March 2015, highlights the increase in the frequency of terrorist incidents around the world, and the number of fatalities associated with such attacks [CMI-1]. In 2013 (the latest year for which published statistics are available) there were nearly 12,000 terrorist attacks in 91 countries – 40% more than in 2012. These resulted in more than 22,000 fatalities. Just over half of all attacks occurred in three countries: Iraq, Afghanistan and Pakistan. As the Report explains:

"The principal threat continues to come from militant Islamist terrorists, notably in Syria and Iraq. ISIL and other terrorist groups in Syria are now supported by foreign fighters from the UK and other European countries. About 6000 people with extremist connections are among the many Britons who have travelled to the region from the UK. Many have now returned here. Some are likely to have received combat experience and other terrorist related training. Terrorism is being fuelled by an unprecedented quantity of extremist and terrorist propaganda."

9. The murder of two British and other hostages in Syria, apparently by a member of ISIL closely connected to the UK, recent terrible events in Paris and Copenhagen and the 31 Britons killed in the attacks of March and June on a Tunisian museum and beach resort, have underlined the threat posed to British nationals – not just in Syria or Iraq but also outside those arenas, including within the EU. In response to the increase in the UK threat level the Government legislated in 2014 to strengthen the UK's capabilities and provided an uplift in counter-terrorism funding including £130m of additional counter-terrorism funding.
10. The task of defending the UK's interests and protecting its citizens in a digital age is becoming increasingly complicated and challenging and it is one in which GCHQ plays a leading role given its expertise in digital communications technology. The evolution of the internet and modern forms of communications are providing terrorists and criminals with new ways to plan direct and increasingly execute their plots. The CONTEST Report notes that ISIL in particular is using social media "... in an unprecedented quantity and frequency, including personalised messages from UK and other foreign fighters and propaganda from the organisation." As Andrew Parker, the Director General of the Security Service (MI5) explained in a public speech to the Royal United Services Institute (RUSI) on 8 January 2015 [CMI-2]:

"It makes full use of the modern social media and communications methods through which many of us now live our lives. By these means it spreads its message of hate directly in to homes across the United Kingdom – both to those seeking it and those who may be susceptible to its distortion and glamorisation of horrific acts".

11. Robert Hannigan, the Director of GCHQ also drew attention in November 2014 to the way in which ISIL is using the internet to "create a jihadi threat with near-global reach" [CMI-3]. In particular:

"[ISIL] also differs from its predecessors in the security of its communications. This presents an even greater challenge to agencies such as GCHQ. Terrorist have always found ways of hiding their operations. But today mobile technology and smartphones

have increased the options available exponentially. Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are "Snowden approved". There is no doubt that young foreign fighters have learnt and benefited from the leaks of the past two years."

12. The diversification of the communications market and the ability of terrorists, criminals and others to exploit new internet-based technologies has made it increasingly difficult for GCHQ and the other intelligence services to monitor the communications of those who present a threat to UK interests. Unless the intelligence services are able to maintain their capabilities in the face of these unprecedented technological challenges, the UK will be unable to obtain the intelligence it needs to counter these threats. As the Chief of SIS made clear in his speech to English Heritage in March 2015, the intelligence services are engaged "... in a technology arms race" [CM1-4].
13. Mr Parker, the Head of MI5, discussed the changing nature of the challenges that the intelligence services face in his BBC interview of 17 September 2015 [CM1-6]:

"We need to be able to use data sets so we can join the dots, to be able to find and stop the terrorists who mean us harm before they are able to bring the plots to fruition. We have been pretty successful at that in recent years but it is becoming more difficult to do that as technology changes faster and faster."

14. The threat to the UK does not stem just from terrorism. For example, as David Anderson QC noted in his independent report on investigatory powers, *A Question of Trust*, [CM1-7], GCHQ used analysis of bulk data to track down two men overseas who had been harnessing the vulnerabilities of the web to blackmail hundreds of children across the world, including the UK, into exposing themselves online – causing them huge trauma. Some of the victims self-harmed and considered suicide. It was the vital work of GCHQ analysts that brought this abuse to an end: they were able to confirm the suspects' names and locations, and to identify an accomplice. After liaison between law enforcement agencies, the two men were arrested and jailed in their home country.
15. But this work tackling national security threats in the digital age is getting harder. One important challenge is the implication of the use of encrypted communications. Encryption is important for computer security and GCHQ advocates its use in the UK as part of good cyber security practice. But the rise of encryption offered by telecommunications companies to their customers has impacted particularly severely on GCHQ's intelligence capabilities because encrypted data acquired lawfully by GCHQ may be unreadable to the intelligence services. The challenges posed by the growth of encryption have become particularly acute over the course of the last two years as telecommunications companies increasingly use improved privacy protections, including encryption by default, as part of their marketing strategies. According to the Director of Europol encryption has now become [CM1-8]:

"... the biggest problem for the police and the security service authorities in dealing with the threats from terrorism... It's changed the very nature of counter-terrorist work from

one that has been traditionally reliant on having good monitoring capability of communications to one that essentially doesn't provide that anymore."

16. The US authorities have experienced similar problems relating to the growth of encryption which they refer to as "Going Dark". The Director of the FBI recently explained [CM1-9]:

"Encryption just isn't a technical feature, it's part of a marketing pitch, but it will have very serious consequences for law enforcement and national security agencies at all levels... There should be no law-free zones in this country..."

17. In a public speech given to RUSI on 10 March 2015, the Foreign Secretary offered a summary of the challenges posed by the accelerating pace of technological change [CM1-10]:

"And as the range of threats gets bigger, so the pace of technological change with which the Agencies must keep pace is getting faster, making their central task of keeping us safe ever more demanding. The Agencies have always had to innovate to stay one step ahead of their adversaries. But the accelerating pace of technological change has upped the ante as terrorists, states and others who would do us harm embrace, adapt, and abuse the technology that we so readily welcome in our everyday lives.

And it is a truism that as technology enables greater productivity, it also open us up to greater vulnerability. So our Agencies must master every technological advance. They must understand its strengths, its weaknesses, the vulnerabilities it introduces – before our enemies can turn it against us".

18. The Security and Intelligence Agencies Financial Statement of June 2014 recognises that the need to maintain capabilities in the face of these rapid technological changes is perhaps the greatest challenge currently faced by the intelligence services [CM1-11].

19. David Anderson QC also highlighted the impact of these challenges in his annual report of the Terrorism Acts (September 2015) [CM1-12]:

"It has been a feature of several major terrorist attacks, including the 7/7 bombings, the killing of Lee Rigby and the French shootings in January 2015, that one or more of the perpetrators was known to the police or security services but had not been assessed as posing a major risk at the time. The speed with which things can change, and the difficulties in knowing how best to prioritise limited surveillance resources, were illustrated in unprecedented detail by the inquiry of Parliament's Intelligence and Security Committee into Lee Rigby's killing."

20. The age of ubiquitous encryption means, inter alia, that GCHQ and the other intelligence agencies require a more innovative and agile set of technical capabilities to meet the serious national security challenges of the digital age. Computer and Network Exploitation (CNE) is one such capability. CNE operations have been authorised by senior Ministers for many years since the 1994 Act, but its importance relative to GCHQ's overall capabilities has been increasing significantly in recent years and is likely to increase further. The allegations made in both claims concern activities known by the

5 of 23

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

intelligence services as CNE, so it is necessary to describe in more detail what CNE operations are.

II. AN OVERVIEW OF CNE AND ITS IMPORTANCE AND VALUE

Computer and Network Exploitation ("CNE")

21. CNE is a set of techniques through which an individual gains covert and remote access to a computer (including both networked and mobile computer devices) typically with a view to obtaining information from it. GCHQ carries out CNE operations as part of its intelligence-gathering activities, as set out below.
22. CNE operations vary in complexity. A straightforward example is the use of the login credentials of a target to gain access to the data held on a computer. The login credentials could belong to a normal user or an entity with elevated privileges such as an administrator.
23. More sophisticated CNE operations involve taking advantage of weaknesses in software. For instance a piece of software may have a "vulnerability": a shortcoming in the coding that may permit the development of an "exploit", typically a piece of software, a chunk of data, or a sequence of commands that takes advantage of the vulnerability in order to cause unintended or unanticipated behaviour to occur. This unanticipated behaviour might include allowing another piece of software – an implant, sometimes called a "backdoor" or a "Trojan" - to be installed on the device.
24. The exploit and subsequent implant can be delivered in a number of ways. Two of the techniques are:
 - a) The user of a device might be sent an e-mail inviting them to open a link or document of interest. When the user clicks on the link or document, it takes them to website that delivers the implant. This is known as "phishing".
 - b) Alternatively, an individual with access to a computer might insert the implant using, for example, a USB stick, whether wittingly or otherwise.
25. The function of an implant may also vary in complexity. A simple implant will typically explore the target computer, sending back information over the internet to its controller. Others might monitor the activity of the user of the target device, or take control of the computer.
26. As with interception, there are a range of circumstances in which a state may require its intelligence services to conduct this type of activity. CNE can be a critical tool in investigations into the full range of threats to the UK from terrorism, serious and organised crime and other national security threats. For example, CNE enables the state to obtain the valuable intelligence it needs to protect its citizens from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality.

27. CNE operations may enable GCHQ to obtain communications and data of individuals who are engaged in activities that are criminal or harmful to national security. Such circumstances may arise where, for example:
- a) the fact that the wanted communications were not in the course of their transmission and could not therefore be intercepted;
 - b) the absence of any Communications Services Providers (CSPs) on whom a warrant can be served to acquire particular communications; and
 - c) the greater possibility of acquiring a comprehensive set of the target's communications/data by means of CNE.

Importance and value of CNE

28. As discussed above, CNE is a critical tool in the investigation of threats to the UK. The UK Government does not have the same ability to identify individuals and entities outside the UK who may pose a threat to national security as compared with those within the UK. Outside the UK, GCHQ's capabilities are the key sovereign intelligence-gathering capabilities available to the Government.
29. Historically, GCHQ's ability to identify individuals of intelligence interest has been based largely on bulk interception. This capability remains critical to the identification and mitigation of threats, but increasingly it is being threatened by the unprecedented technological challenges outlined in part (I) of my statement. As the Foreign Secretary explained in his speech to RUSI:
- "...And to GCHQ, although since its birth a signals intelligence organisation, the rapid pace of the development of the internet and the sheer scale of its traffic, pose new challenges – finding the needle of vital information to safeguard our security in a hay stack that is growing exponentially and is already well beyond the capacity of human analysis."
30. As noted in the previous section, the introduction of strong encryption across many web services in the wake of the Snowden allegations has posed particular technological challenges. The spread of encryption has impeded intelligence service access to communications. In his own speech to RUSI on "terrorism, technology and accountability, Andrew Parker, the Director General of MI5 said:
- "Changes in the technology that people are using to communicate are making it harder for the Agencies to maintain the capability to intercept the communications of terrorists. Wherever we lose visibility of what they are saying to each other, so our ability to understand and mitigate the threat that they pose is reduced."
31. In the light of these developments, CNE is increasingly required to enable GCHQ to continue to obtain the intelligence the Government requires to identify individuals outside the UK who may pose a threat to national security. Indeed CNE may in some cases be the only way to acquire intelligence coverage of a terrorist suspect or serious

criminal in a foreign country. As noted by the Intelligence and Security Committee at page 67 of its Privacy and Security Report [CM1-13]:

"During 2013 a significant number of GCHQ's intelligence reports contained information that derived from IT operations against a target's computer or network....."

32. At the same time as GCHQ is adapting to meet these new technological challenges, there is an increasing expectation within Government that GCHQ will play a lead role in improving cyber security for the protection of the UK's vital national interest in an era where threats to the UK from cyber space are growing very rapidly. GCHQ plays a key role in securing the safety of the internet for the benefit of the public as I explain further below. CNE is an important part of GCHQ's ability to understand, detect and disrupt cyber threats to the UK.
33. GCHQ's CNE capabilities have made a vital contribution to counter the increased threat to the UK from militant Islamist terrorists. And, as noted in the previous section, GCHQ's CNE capabilities have also enabled the disruption of paedophile-related crime. I cannot say more about these operations in this open, public statement without undermining the interests of national security and the prevention and detection of serious crime.
34. CNE has long been an essential part of GCHQ's capabilities. It has become increasingly important in recent years and will become more important yet in the years ahead. Without it, GCHQ's ability to protect the public from terrorism, cyber attack, serious crime, including child sexual exploitation, and a range of other threats would be seriously degraded.

The Claimant's allegations about CNE

35. The Claimants make a number of general and specific allegations in the two Claims. Before addressing the specific allegations made by the Complainants, I would like to make four preliminary points in relation to the general allegations.
36. First, the Claimants allege that the tools used by GCHQ allow huge amounts of information (current and historical) to be extracted from "millions" of devices thereby subjecting users to mass and intrusive surveillance. Allegations that GCHQ conducts "mass surveillance" were made by one of the Claimants in the context of a previous complaint before this Tribunal. On that occasion the Tribunal stated "we are entirely clear that the Respondents are not seeking, nor asserting that the system entitles them to seek, to carry out what has been described as "mass" or "bulk" surveillance". I should like to make clear that it is equally the case that GCHQ neither seeks, nor believes that we are entitled to seek to carry out indiscriminate mass surveillance activities of the sort alleged in this case. They are also precluded by the clear statutory framework which regulates GCHQ's activities. CNE must be authorised by a Secretary of State and is subject to strict tests of necessity, proportionality and legitimate aim as set out in the Intelligence Services Act 1994. These authorisations, and the internal processes that GCHQ has in place to manage the authorised activities, are subject to independent scrutiny by the Intelligence Services Commissioner. In February 2015, the Government published a draft Equipment Interference Code of Practice. It set out the strong

safeguards that GCHQ has always applied to CNE activities. More generally, any conduct by GCHQ must be consistent with its statutory functions and the purposes for which those functions may be exercised. As the ISC has recently made clear in its report on Privacy and Security:

“We are satisfied that the UK’s intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do.”

37. It follows that a significant proportion of the examples given in the Claimants’ evidence with respect to the possibilities created by CNE tools bear no relation to the reality of GCHQ’s activity and/or would be unlawful having regard to the relevant statutory regime.
38. Secondly, the Claimants allege that CNE may create potential security vulnerabilities or leave users vulnerable to further damage.
39. Intelligence work by its nature is secret – both the how and the specific targets. It is therefore in GCHQ’s interests to carry out CNE operations in such a way that the activity is not apparent to the target, nor to others wanting to know who the specific targets of HMG intelligence activities are. GCHQ does not intrude into privacy any more than is necessary to discharge our functions. Nor would it be right to enable others to intrude into privacy. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon. It would also increase the risk of those who wish to know who our targets are identifying GCHQ’s tools and techniques. Operations are therefore carried out in such a way as to minimise that risk.
40. I should also like to take this opportunity to explain GCHQ’s role more generally in securing the safety of the internet for the benefit of the public. The internet is an intrinsically insecure environment, with billions of computers constantly running millions of complex programmes. PwC’s 2015 Information security breaches survey [CM1-5] reported that 90% of large organisations and 74% of small businesses had a security breach in the period covered by the report; the average cost of the worst serious breach ranged from £1.46m to £3.14m for large organisations; £75,000 to £311,000 for small businesses. GCHQ’s role is to play its part in helping to make the internet as safe as possible for ordinary citizens and legitimate businesses, and prevent its use by criminals and terrorists. We engage with strategically important organisations who are particularly vulnerable to cyber attack, and we also promote high standards of cyber security across all sectors of the UK, including by recommending the use of strong encryption.
41. One element of GCHQ’s information assurance work concerns the finding and reporting of vulnerabilities in digital technologies. GCHQ helps technology providers identify weaknesses in finished hardware and software; we also help uncover potential issues at the design stage, often before they become major in-service problems – saving firms time and money. Some but not all vendors choose to publicly credit GCHQ for finding those weaknesses. For example, in September of this year, Apple publicly credited CESG, the Information Security arm of GCHQ, with the detection of a vulnerability in their iOS operating system which could have been exploited to allow the unauthorised modification of software on devices such as iPhones and iPads, the extraction of information from

9 of 23

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

those devices, or to disrupt their operation. That vulnerability has now been patched. In the last two years, GCHQ has disclosed vulnerabilities in every major mobile and desktop platform, including the big names that underpin British business.

42. Thirdly, while CNE operations can be highly intrusive, they are not in general any more intrusive than any other operations conducted by GCHQ under the Regulation of Investigatory Powers Act 2000 ("RIPA") or the Intelligence Services Act 1994 ("ISA").
43. By way of example, Part II of RIPA permits certain public authorities to authorise intrusive surveillance in relation to residential premises and private vehicles. A listening device located within a private address - potentially including a bedroom - clearly has the potential to obtain private information relating to all the occupants of that address (including non-targets) of an extremely sensitive and personal nature. Information of this nature which is communicated between two or more people within a residential address or a private vehicle may well contain content that those individuals would deem too personal, private or sensitive to commit to writing and store on a device. Nonetheless, such highly intrusive surveillance is lawful if properly authorised, having met the tests of necessity and proportionality.
44. Similarly, while CNE operations can be used to access a wide range of data, they are not in general any more intrusive than the interception of communications under Chapter I of Part I of RIPA. With the advent of Cloud storage (which many people opt to use), all the material referred to by the Claimants in their complaints would be potentially available to the intercepting agencies via interception - including photographs, videos, passwords, banking details, passport details, etc. All of this material could, in principle, be acquired by way of interception.
45. In summary, while the level of intrusiveness will clearly vary depending on the type of activity in issue, I do not therefore believe it is the case that GCHQ's CNE operations are in general any more intrusive than its other operations involving interception, surveillance or other investigative techniques.
46. Fourthly and finally, GCHQ recognises that CNE activity could theoretically change the material on a computer. For example the installation of an implant would itself amount to a change. However it would be neither necessary nor proportionate, nor would it be operationally sensible, for an organisation seeking to use CNE for intelligence gathering purposes to make more than the most minimal, and to the greatest extent possible, transient, changes to targeted devices.

III. SAFEGUARDS AND OVERSIGHT MECHANISMS

Overview

47. The regime governing GCHQ's CNE activities consists of provisions in primary legislation and in relevant Codes of Practice and also in relevant internal arrangements and safeguards which are applied by GCHQ.

48. I explain below the key components of the application process for CNE warrants and authorisations, and the oversight arrangements governing GCHQ's CNE activities. These processes are supplemented by the Equipment Interference Code of Practice [CM1-14] which contains important safeguards including:

- a) Detailed guidance on the requirement of proportionality and the considerations which apply in the CNE context, including issues such as collateral intrusion and the need to consider less intrusive alternatives (Chapter 2);
- b) Guidance on the frequency of reviews, particularly where there is a high level of intrusion into private life or significant collateral intrusion or confidential information is likely to be obtained (Chapter 2 at §§2.13-2.15);
- c) Best practice guidance on applications for warrants/authorisations (§§2.16-2.17);
- d) Special considerations which should apply to legally privileged and confidential information (Chapter 3);
- e) Detailed and comprehensive procedures for the authorisation of both sections 5 and 7 ISA equipment interference activity (see Chapters 4 and 7);
- f) Important record keeping requirements in respect of any CNE (Chapter 5);
- g) Comprehensive safeguards and guidance as regards the processing, retention, disclosure, deletion and destruction of any information obtained by the intelligence services pursuant to interference CNE warrant, which mirror similar safeguards applied as part of the interception regime pursuant to section 15 of RIPA (Chapter 6).

49. GCHQ's internal arrangements are safeguards set out in the Respondents' Closed Response and Closed witness evidence. I also refer to certain of the internal arrangements in this statement. They include the Compliance Guide, which is a document which is made available electronically to all GCHQ staff. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity be:

- a) Authorised (generally through a warrant or equivalent legal authorisation);
- b) Necessary for one of GCHQ's operational purposes; and
- c) Proportionate.

49A. These principles and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.

49B. In addition, pursuant to GCHQ's Compliance Guide and Intelligence Sharing and Release Policy (a policy document governing the sharing and release of operational data), the position is that all operational warrant is handled, disclosed and shared as

though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

- 49C. GCHQ's internal arrangements also address the role of the Reporting Quality Checker in ensuring that any release of intelligence outside of GCHQ is lawful and proportionate.
- 49D. GCHQ has a collaborative relationship with the NSA. Activities forming part of that relationship must be undertaken in accordance with the principles set out in the Compliance Guide, which emphasises the need for all operational activity to be necessary and proportionate.

Authorising CNE: section 5 and 7 ISA

50. GCHQ conducts all CNE activity pursuant to warrants under section 5 of the ISA or authorisations under section 7 of the ISA. I have set out below an explanation of the differences between the section 5 ISA regime and the section 7 ISA regime as it applies to GCHQ's activities. I have also identified the detailed safeguards which regulate this activity including:

- a) The processes for applying for, renewing and cancelling section 5 warrants;
- b) The processes for gaining section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals;
- c) Oversight by the Intelligence Services Commissioner;
- d) Oversight by the Intelligence and Security Committee of Parliament (ISC).

51. These safeguards and oversight mechanisms are reflected in the Covert Surveillance and Property Interference Code and the draft Equipment Interference Code of Practice

a) The processes for applying for section 5 warrants

52. The section 5 ISA regime is used primarily by GCHQ to authorise CNE operations against specific equipment located within the UK. Section 5(2) of ISA provides that the Secretary of State may, on an application made by GCHQ, issue a warrant authorising the taking of action in respect of property as specified in that warrant if he: thinks it necessary for the action to be taken for the purpose of GCHQ in carrying out any function that falls within section 3(1)(a) of ISA; is satisfied that the taking of action is proportionate to what the action seeks to achieve; and is satisfied that satisfactory arrangements are in force under section 4(2)(a) of ISA with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements.

53. Applications for section 5 warrants in respect of CNE must contain all the detailed matters as set out in paragraph 4.6 of the current draft Equipment Interference Code of Practice. Prior to the publication of this draft Code of Practice on 5 February 2015 applications were required to conform with paragraph 7.37 of the Covert Surveillance and Property Interference Revised Code of Practice published on 10 December 2014 [CM1-15]. This required GCHQ to provide the same information in support of an application as

would be required when the police, the services police, National Crime Agency (NCA), HM Revenue and Customs (HMRC) or Competition and Markets Authority (CMA) were making an application to an authorising officer. The details of this information are set out in paragraph 7.18 of the Surveillance and Property Interference Revised Code of Practice. These requirements (and the numbers of the relevant paragraphs) were unchanged from previous versions of the Code of Practice published in [2000] and revised in 2010.

- 53A. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

"A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ official of appropriate seniority if a Secretary of State has expressly authorised its use."

- 53B. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants ("the Section 5 Guidance"). This was updated in January 2015. The internal guidance is regularly reviewed to ensure that it remains comprehensive and pertinent as GCHQ's CNE activities continue to evolve. The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target's privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

b) The processes for applying for section 7 authorisations, including the processes for Secretary of State authorisation and for internal approvals

The importance of CNE as an overseas intelligence gathering capability

54. As I have already explained, the UK Government does not have the same ability to identify individuals outside the UK who may pose a threat to national security as compared with those within the UK. Outside the UK, GCHQ's capabilities are the key sovereign intelligence-gathering capabilities available to the Government.
55. There are important practical differences between gathering intelligence on individuals, organisations and equipment within the UK and gathering intelligence on individuals, organisations and equipment that exist or operate outside that jurisdiction. These

practical differences are reflected in the authorisation regimes provided by sections 5 and 7 of the ISA.

56. As mentioned above, the section 5 ISA regime is used primarily by GCHQ to authorise CNE operations against specific equipment located within the UK. By contrast, section 7 permits the giving of class authorisations which do not require the authorisation to name or describe a particular piece of equipment, or an individual user of the equipment. Consequently CNE is authorised in relation to equipment located outside the UK pursuant to a section 7 class authorisation and internal approvals. This reflects practical realities of intelligence gathering outside the UK, where GCHQ requires the flexibility to obtain material which will contain intelligence relevant to the safeguarding of the UK's national security without knowing in advance from which particular piece of equipment that material may be obtained.
57. In line with the foregoing, a class authorisation under section 7 ISA is sought wherever members of GCHQ conduct CNE in relation to equipment located outside the UK that would otherwise be unlawful. This includes cases where the act is done in the UK, but is intended to be done in relation to apparatus that is or is believed to be outside the UK, or in relation to anything appearing to originate from such apparatus. In addition GCHQ will obtain a section 7 authorisation for any CNE activities carried out abroad or over a foreign computer, even if the relevant user is located in the UK. Paragraph 7.4 of the current draft Equipment Interference Code of Practice sets out the additional safeguards which apply if either the subject of a section 7 operation is known to be in the UK, or the equipment is brought to the UK during the currency of the authorisation.
58. While GCHQ's section 7 CNE class authorisation offers the potential for broader and more flexible acquisition of intelligence than is permitted under its section 5 warrants, the process described below for giving section 7 authorisations, in combination with GCHQ's system of internal approvals and additions, ensures that its activities are properly regulated and subject to strict safeguards and oversight.

Section 7 authorisations

59. Section 7 ISA provides that an authorisation has to be issued personally by the Secretary of State on an application to him to that effect. The purposes for which warrants are issued are set out in section 7(3) ISA.
60. Section 7(1) of ISA provides that a person shall not be liable in the United Kingdom for any act done outside the UK for which he would be liable, if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under that section.
61. Paragraph 7.1 of the current draft Equipment Interference Code of Practice requires that GCHQ applies the provisions of that Code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of ISA. Paragraph 7.7 of the current draft Equipment Interference Code of Practice states that an application for the giving or renewal of a section 7 authorisation should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 CNE warrant.

62. Paragraph 7.11 of the current draft Equipment Interference Code of Practice states that an authorisation under section 7 may relate to a broad class of operations. Paragraph 7.12 states that where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of CNE must be sought from a designated senior official. In any case where the CNE activity may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer (and in the case of GCHQ an Annex A approving Officer is someone in a small group of GCHQ's most senior managers).
63. Applications for section 7 authorisations must, as far as is reasonably practicable in the circumstances, contain all the detailed matters set out in paragraph [4.6] of the EI Code. The process by which GCHQ obtains Secretary of State authorisation for class authorisations under section 7 of the ISA has evolved over the last few years with an increasing emphasis on providing detailed information to the Secretary of State about the type of CNE activities covered by the class authorisation. Since July 2014 GCHQ has copied to the FCO all of its internal section 7 approvals for CNE operations which were given pursuant to the class authorisation. In August 2013 GCHQ recommended that, in future, the internal approvals should be sent through the relevant department in the FCO to the Secretary of State and this was agreed by the FCO.

Internal approvals

64. Where a class authorisation has been given by the Secretary of State under section 7, internal Approval to conduct individual operations under that authorisation in respect of CNE must also be sought from a designated senior official.
65. Before granting an approval, the senior official must be satisfied that the proposed operations are necessary, proportionate and within the scope of the class authorisation. Approval may only be given where operations are necessary in the interests of national security, for the prevention and detection of serious crime or in the interests of the economic wellbeing of the UK. In addition, the senior official must be satisfied that the nature and degree of the proposed intrusion against target computers is proportionate and limited to that required for the operation to be effective, and that safeguards are in place to ensure that any aspect of the operation or the data thus obtained is handled in a manner consistent with GCHQ's legal obligations under Intelligence Services Act and the Human Rights Act. Feeding into the internal approvals process is an internal specialist risk assessment panel, involving a range of relevant technical, operational and policy leads. This panel provides expert oversight and assurance to operators, policy leads and senior leadership that the tools and techniques being used, and the way in which they are being used, present an acceptable level of technical and operational risk. Key agreements and decisions made by the internal specialist risk assessment panel are documented. They provide an audit trail and a 'history' of decisions (which, for example, are used to inform risk assessment statements made in section 7 approval requests and political submissions).
66. GCHQ copies to the Foreign and Commonwealth Office all of its internal s.7 approvals and extensions for CNE implant operations which were given pursuant to the class

authorisation. In addition, if an operation is judged to present significant risk, the proposal will be submitted to FCO officials or the Secretary of State (and GCHQ will also seek FCO legal advice if a proposed operation involves issues of international law).

66A. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an "addition" to an existing approval is required.

Additions

67. Under an internal approval, operations against specific targets are authorised by means of an 'addition'. The term "addition" is not specifically defined in GCHQ's internal arrangements, but is used within GCHQ to refer to the process and associated formal documentation for the inclusion of further specific targets within the scope of an existing internal approval for a CNE operation. The "additions form" requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

68. The level of detail in an addition will be tailored to the operation in question, but it will describe the specific target (which must fit within the description of the target set in the relevant internal approval) and the necessity and proportionality of the planned operation, as well as how intrusion into privacy will be managed. The addition will also describe the planned activity and assess the risks associated with this (which must fit within the thresholds set in the relevant internal approval). The role and seniority of the authoriser for additions depends on factors including the sensitivity and complexity of the planned activity, but the authoriser must always have been trained before assuming the role.

68A. Analysts will have assigned to them a point of contact within the CNE operational team with whom they can speak about operational matters. In addition, within their own team they will have a dedicated point of contact with whom they can discuss any legal and policy questions.

Records

68B. GCHQ creates and maintains records of the application for, renewal of, approval of and cancellation of all warrants under section 5 and class authorisations and internal approvals under section 7 indefinitely. These include any comments or stipulations from the Secretary of State relating to them.

Training

68C. GCHQ has a comprehensive programme of training and testing in place for those involved in CNE operations and for intelligence analysts who may have access to data obtained in CNE operations. This training includes operational and mandatory legalities training. The training involves testing and regular reassessment.

c) Oversight by the Intelligence Services Commissioner

The Commissioner

16 of 23

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

69. GCHQ's CNE operations are overseen by the Intelligence Services Commissioner under section 59(1) of RIPA. The Rt Hon Sir Mark Waller currently holds this role and he was appointed by the Prime Minister on 1 January 2011. His predecessor was Sir Peter Gibson (also a former Lord Justice of Appeal).

70. The functions of the Intelligence Services Commissioner, as they relate to CNE, are:

- a) To keep under review the exercise by the Secretary of State of his powers to issue, renew and cancel warrants under sections 5 and 6 of ISA;
- b) To keep under review the exercise by the Secretary of State of his powers to give, renew, and cancel authorisations under section 7 of ISA;
- c) To give the Tribunal all such assistance (including my opinion on any issue falling to be determined by it) as it may require in connection with its investigation, consideration or determination of any matter;
- d) To make an annual report to the Prime Minister on the carrying out of my functions, such report to be laid before Parliament.

71. The Intelligence Services Commissioner formally inspects GCHQ's CNE activity twice a year, and also makes ad hoc visits to look at particular aspects of its work in more depth. These are known as 'under the bonnet' visits. During the formal inspections the Commissioner raises inquiries, examines procedures and examines the relevant paperwork for a selection of warrants, class authorisations (including internal approvals and relevant additions), that he personally has chosen in advance, to ensure that it is in order and that, in particular, sufficient consideration has been given to issues like collateral intrusion and privacy. In order to permit the Commissioner to make a selection of the documents he wishes to see, GCHQ provides him with a "choice letter" containing:

- a) Summaries of all section 5 ISA warrants and section 7 ISA class authorisations that are either in place or which have been cancelled or allowed to expire since the previous choice letter, including all internal approvals underneath the latter. Those warrants and class authorisations that the Commissioner has previously inspected are flagged as such;
- b) A list of errors reported to the Commissioner since the previous Review;
- c) A list of intelligence reports at least partially sourced from CNE operations, which contain confidential or legally privileged material issued since the previous choice letter;
- d) A list of all warrants and authorisations examined at previous reviews by the current Commissioner.

71A. As part of the **September 2010** visit, Sir Peter Gibson discussed a recently reported CNE error which led to a change being made in warrant applications.

71B. During Sir Mark Waller's visit in **March 2011** he commented on the section 7 approvals and noted that 'proportionality' appeared in its own right on the section 7 approval form, but would have liked to see 'necessity' appear in its own right on the form. This change was subsequently introduced.

- 71C. During the **December 2013** Inspection the Commissioner expressed himself content with the actions GCHQ had taken in respect of documenting privacy considerations in warrant and authorisation application paperwork since June 2013.
- 71D. Following the discovery of a typographical error relating to the expiry date of the renewal of a section 5 warrant the Commissioner had asked that the Secretary of State amend the face of the instrument in his own hand and initial the change. The Commissioner queried why the error had not been picked up sooner and asked to see a copy of the checklist that is used to check warrants before they go up to FCO. He asked that the list be supplemented with a further check to be carried out when the signed warrant is returned from the warrant issuing department to ensure that any future mistakes are picked up at an early stage. He also asked to be informed if there were any similar instances in the future and this was agreed.
- 71E. There was also a discussion of what information should be included on warrant renewal instruments. It was explained that, until recent years, renewal instruments for section 5 warrants had contained the minimum wording stipulated by ISA section 6. GCHQ had subsequently added a description of the property (which made it easier to see to what a renewal instrument referred), and, prompted by the Commissioner, had then added a final paragraph reminding the Secretary of State of his statutory obligations when signing the renewal. The Commissioner's view was sought as to whether it would be helpful to add a description of the actions authorised by the warrant. Sir Mark felt that, if we were minded to make further changes to the renewal instrument, we might consider including all the relevant wording from the original instrument.
- 71F. In the **May 2014** Inspection the Commissioner recommended a new form of words for section 5 warrants which make clear that the Secretary of State is authorising on the basis that GCHQ will act in accordance with the accompanying submission. He also made recommendations about the conditions set out in the submissions and instruments. He continued to monitor thematic property warrants closely.
- 71G. In the **November 2014** Inspection the Commissioner expressed himself content that GCHQ record on the warrant instrument that we will comply with any conditions set out in the accompanying submission as this formally joins the warrant to the submission.
- 71H. There was also discussion about section 5 ISA warrants that are "thematic" rather than relating to specific property. The Commissioner asked that section 5 warrants should relate to specific property wherever possible rather than relying on a thematic warrant. Overall the Commissioner indicated that he was content for such warrants to be used, where there is no intrusion into privacy, but emphasised that they should be the exception and not the rule.
- 71I. The Commissioner's **April 2015** Inspection was the first inspection at which the Commissioner formally inspected the Additions layer (under internal approvals) for the s.7 authorisations process. As already set out above, this is the layer at which individual targets are usually described. The Commissioner recommended changes be

made to ensure that each element is dealt with explicitly and at the earliest opportunity. These changes have been implemented.

- 71J. Sir Mark Waller has conducted a number of what he refers to as “under the bonnet” visits, separate from his formal inspections.
- a) On 20 January 2012 Sir Mark was briefed on GCHQ’s CNE activities.
 - b) On 10 July 2013 Sir Mark sat in on one of the legalities courses.
 - c) On 11 September 2014 Sir Mark visited GCHQ following an approach to him by a BBC journalist, following media reports about certain alleged CNE activities.
- 71K. The Commissioner’s most recent “under the bonnet” visit was on 9 December 2014. This visit was intended to give him an overview of GCHQ’s operational use of CNE so that he could see how our internal governance processes meshed with the authorisation regime. During the visit we established that Sir Mark fully understood the section 5 authorisation regime, so the focus was primarily on operational activity authorised under ISA s.7, and how GCHQ used its internal hierarchy of approvals and additions. Sir Mark was briefed on the internal approvals process, and the circumstances where GCHQ would seek political approval for activities.
- 71L. I am aware that the Intelligence and Security Committee of Parliament, in their report of 12 March 2015, “Privacy and Security: A modern and transparent legal framework”, addressed section 7 authorised operations at paragraphs 177ff and said this at Recommendation BB on page 66:

“While intrusive action within the UK requires a Ministerial warrant, outside the UK it is authorised by the use of a Class Authorisation under the Intelligence Services Act 1994. However, the Agencies do not all keep detailed records of operational activity conducted under these Class Authorisations. It is essential that they keep comprehensive and accurate records of when they use these powers. It is unacceptable not to record information on intrusive action.”

Given the Commissioner’s clear endorsement of GCHQ’s internal section 7 processes and the associated record keeping undertaken by GCHQ (the “audit trail” in the Commissioner’s words), I do not consider that this statement relates to GCHQ’s CNE operations. As set out earlier in this statement GCHQ does keep very detailed records of CNE activity conducted pursuant to section 7 authorisations, including all details of internal Approvals and Additions.

- 71M. Finally, it is to be noted that we have an established process for reporting errors to the Commissioner. In particular error reports follow a standard structure with sections addressing:
- o The background;
 - o How and why was it identified?
 - o What was the magnitude of the error?
 - o Why did this happen?
 - o How we’ll make sure it never happens again.

19 of 23

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

Reports of the Commissioner

72. In his formal reports, the Commissioner has explained the extent of his oversight of GCHQ's CNE activities and made a number of positive comments about GCHQ's CNE operations and the thoroughness of its processes. In his report for 2013 [CM1-20] the commissioner stated:

"From my work it is clear to me that GCHQ apply the same human rights considerations and the same privacy considerations, checks and balances to the virtual world as they do to the real world. From my scrutiny of GCHQ authorisations, inspection visits and my under the bonnet work, it is my view that GCHQ staff continue to conduct themselves with the highest level of integrity and legal compliance."

- 72A. In his Report for 2014 [CM1-16] the Commissioner explained the nature of his review functions and highlighted the extent of co-operation which he received from the Agencies in this regard. He stated:

"I emphasise that I do this activity personally and I undertake my duty rigorously and entirely independently of government, Parliament and the intelligence agencies themselves, without political favour or personal bias..."

"A duty of cooperation is imposed on every member of every agency, every departmental official and every member of the armed forces to disclose or provide to me all such documents and information as I may require. I have never had anything but cooperation in this regard."

- 72B. In the same report he commented on GCHQ's record keeping in terms of warrantry and authorisation:

"GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips."

- 72C. The Commissioner also noted that he had spent a day at GCHQ looking at the system by which GCHQ manages its internal approvals and additions, and questioning the staff who undertake the approvals and the CNE activity, in order to understand what consideration was being given at each stage of the process to protecting privacy, and what was done with any product from CNE operations. The Commissioner concluded:

"My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration that was given to each operation; it was clear to me that a great deal of thought was going into the process..."

"GCHQ primarily operate under class authorisations and have very few specific section 7s. They provide for my oversight the internal approvals they make under each class authorisation and have implemented my recommendation to ensure that the paperwork reflects that these approvals are only valid as long as the class authorisation is in place. They are approved by a GCHQ senior official but if there is any additional sensitivity or

political risk it will only be signed after a senior Foreign Office official or the Foreign Secretary has been consulted and agreed the operation is appropriate. I have made it clear that the senior official cannot authorise necessity and proportionality; this decision must be made by the Secretary of State and cannot be delegated."

"GCHQ's internal approvals are supplemented by what they call an "addition". To help me gain a better understanding I spent a day in GCHQ:

- Looking more closely at the system;
- Questioning the staff who undertake the approvals; and
- Questioning the staff who undertake the activity."

"I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion."

"I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I recommended that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ."

73. This recommendation has been implemented.

d) Oversight by the Intelligence and Security Committee of Parliament

The Committee

74. GCHQ is responsible to the Secretary of State for Foreign and Commonwealth Affairs. The Secretary of State is in turn accountable to Parliament. Parliamentary responsibility for scrutiny of the activities of GCHQ falls principally to the Intelligence and Security Committee of Parliament ("the ISC").
75. The ISC, in its original form, was established by the Intelligence Services Act 1994. On 25 June 2013 the ISC was reconstituted under the Justice and Security Act 2013 ("the JSA"). From that date onwards the JSA has provided the governing statutory framework for the ISC. In its annual report for 2012-2013 [CM1-17], the ISC stated that it welcomed the changes in the JSA and that those changes were "broadly in line with those which we ourselves had previously recommended to the Government, and which will increase accountability" (at page 83).
76. The ISC operates within the "ring of secrecy" which is protected by the Official Secrets Act 1989. It may therefore consider classified information, and in practice takes oral evidence in open and closed session from the Foreign and Home Secretaries, the three heads of the intelligence services, and their staff.
77. The heads of the intelligence services are under a general obligation to arrange for any information requested by the ISC in the exercise of its functions to be made available to it. The power to refuse such a request has been removed from the heads of the

21 of 23

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306, email infoleg@gchq.gsi.gov.uk

intelligence services and now lies with Ministers alone, who can only exercise this power in certain limited circumstances.

78. In order to be able effectively to carry out its expanded remit under the JSA, the ISC's budget has been substantially increased and the ISC is in the process of recruiting further staff. This will result in a three-fold increase in the ISC's investigative capacity.

Privacy and Security: A modern and transparent legal framework

79. The ISC sets its own agenda and work programme. Following the Snowden allegations in the summer of 2013, the ISC decided to investigate an allegation made in some of those reports to the effect that GCHQ had acted illegally by accessing communications content via the US PRISM programme. On 17 July the Committee made a statement [CM1-18] which concluded that the allegation that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications was unfounded. They also concluded that it would nevertheless be proper to "... consider further whether the current statutory framework governing access to private communications remains adequate."

80. On 17 October 2013, the ISC announced that it would be broadening this review of the legislative framework governing the intelligence services' access to the content of private communications to consider, additionally, the appropriate balance between privacy and security in an internet age [CM1-19]. The result of this review, *Privacy and Security: A modern and transparent legal framework*, was published on 12 March 2015 [CM1-13]. Paragraph v of the introduction to the review says:

"Our Inquiry has involved a detailed investigation into the intrusive capabilities that are used by the UK intelligence and security Agencies. This Report contains an unprecedented amount of information about those capabilities, including how they are used, the legal framework that regulates their use, the authorisation process, and the oversight and scrutiny arrangements that apply."

81. The Committee's first key finding reads:

"We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do."

82. In the report the Committee also indicated that it had been informed about the full range of Agency capabilities, how they are used and how they are authorised.

Conclusion

83. In this statement I have endeavoured to the best of my ability and knowledge to:

- describe the range of serious national security threats faced by the UK and its people to which GCHQ is required to assist in defending against;

- set out the requirement for Computer and Network Exploitation (CNE) capabilities to help us counter these threats, principally international terrorism, cyber attack (including from hostile state actors), and serious crime (including child sexual exploitation);
- give an account of the robust procedures for the use of GCHQ's CNE capabilities, and summarise the result of various Parliamentary, judicial and other inquiries and inspections which shows GCHQ's adherence to these strict procedures;
- describe the growing importance of CNE to the protection of the UK. Whilst it has been an important GCHQ capability for many years, its importance has been growing and is set to grow further, partly because of the growth of ubiquitous encryption which has affected GCHQ's ability to collect data for intelligence purposes by other means. It is therefore the case that without CNE capabilities GCHQ's ability to protect the British public from terrorism, cyber attack, online child sexual exploitation and a range of other serious crime would be badly diminished.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed:*[Signature]*.....

Dated: 16 November 2015

o

o

Statement No 2
For the Respondents
Dated 23 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/14/85/CH

PRIVACY INTERNATIONAL

Claimant

-and-

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS
- (2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/120-126/CH

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS
- (2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

SECOND WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

- 1) I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also have wider responsibilities for GCHQ's external communications and policy. I have been in

this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

- 2) This is my second witness statement in these proceedings which I am authorised to make on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.
- 3) Attached to this statement and marked Exhibit ['CM2'] is a bundle of relevant documents. Tab and page numbers below are references to that Exhibit.
- 4) In this second statement I address GCHQ's safeguards for communications protected by legal professional privilege ("LPP") and other confidential communications.

LPP and confidential communications

- 5) The RIPA Interception of Communications Code of Practice and the draft Equipment Interference Code of Practice stipulate that particular consideration should be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information (such as that which is legally privileged) is involved. GCHQ therefore takes special care to ensure that the acquisition, analysis and retention of communications in these circumstances, and the dissemination of any intelligence produced from them, is necessary and proportionate.
- 6) GCHQ treats four main categories of material as requiring special handling and dissemination; material that is legally privileged, confidential personal information, confidential journalistic information and the communications of and with UK legislators.
- 7) GCHQ applies those safeguards and handling procedures in place to ensure compliance with the RIPA Interception of Communications Code of Practice to all its data, irrespective of origin. Therefore, GCHQ's policies are applicable across the board, and apply equally to data derived from Computer Network Exploitation (CNE) as they do to data derived from other forms of interception.
- 8) A number of different GCHQ policies are relevant to the interception of legally privileged communications.
- 9) Acting on the advice of Counsel to Her Majesty's Government (HMG), and following the Belhaj IPT complaint, GCHQ's policies on the interception and reporting of legally

privileged communications were updated in the first half of 2015. In June 2015 the Interception of Communications Commissioner's Office (IOCCO) was consulted on these changes, and by August 2015 the policies had been further amended to incorporate suggestions made by IOCCO.

- 10) A copy of the 'Targeting' section of GCHQ's Compliance Guide is attached at [CM2-1]. This contains guidance where there may be targeting of lawyer's communications. This requires that "careful consideration" is given where lawyer-client communications are targeted. The 2015 changes to the policies on the interception and reporting of legally privileged communications stipulate that if officers intend to carry out any targeting that may attract any of the four categories of sensitive communications, (including those of a lawyer), an internal authorisation (a Combined Policy Authorisation (COPA)) must be obtained. In particular, where legally privileged information is or is likely to be involved, this authorisation must be ratified by a senior Foreign and Commonwealth Office (FCO) official prior to its approval within GCHQ.
- 11) Further information is provided in the 'Communications containing Confidential Information' section of the Compliance Guide (see attached at [CM2-2]). This document contains stipulations which are necessary in order to comply with the requirements of the Code of Practice where material which is legally privileged may be intercepted. This makes expressly clear that no material should be transcribed, gisted or otherwise analysed unless there are reasonable grounds to believe that it is necessary on the grounds of national security, the economic well-being of the UK or preventing or detecting a serious crime (see page 3 of [CM2-2]). It also states that intelligence based on the interception of confidential information can only be disseminated in accordance with GCHQ Reporting Policies on the sensitive professions and proportionality. Any intelligence that may potentially be confidential must be submitted for mandatory sensi-check. Staff other than those in the relevant GCHQ team are not empowered to release such information themselves unless as per agreement with the relevant GCHQ team.
- 12) As of April 2015 it specifies in the 'Communications containing Confidential Information' section of the Compliance Guide that if officers are likely to obtain confidential information as a result of their targeting activities, they must obtain a COPA in advance. This directive reasserts that in the case of legally privileged information, the COPA must be ratified by a senior FCO official.
- 13) The 'Oversight' section of the Compliance Guide (see [CM2-3]) explains that both the Intelligence Services Commissioner and the Interception of Communications Commissioner have oversight of the Intelligence Agencies' activities in respect of the four categories of communications containing confidential information, as specified above. Warrants and reporting that relate to communications containing confidential information will explicitly be

brought to the attention of the relevant Commissioner during the next inspection visit. Any material containing confidential communications that is retained will be made available to the relevant Commissioner if requested, including detail of whether that material has been disseminated.

- 14) GCHQ's Intelligence Sharing and Release Policy (see [CM2-4]) which came into force in September 2013 and was updated in June 2015 contains further guidance on the RIPA Code of Practice, the Human Rights Act 1998 and confidential communications. This document explains legal privilege and makes clear that such communications attract a special sensitivity. Any such material must undergo a mandatory sensitivity check (referred to as a sensi-check in the guidance). This check is done by a team separate from the team dealing with reporting. If in a particular case it is proportionate to release legally privileged material, the reporter will be instructed to apply the following caveat to the report, to help demonstrate that GCHQ has taken account of the communications' sensitivity and the heightened threshold of proportionality:

"This report contains material that may be subject to legal professional privilege, and onward dissemination/Action On is not to be taken without reverting to GCHQ."

- 15) The Intelligence Sharing and Release Policy sets out how the process of sensi-checking should be conducted. It also makes clear that communications of, and as of 2015, mention of sensitive professionals including lawyers or legal advisers are subject to a mandatory sensi-check. Prior to the creation of the Intelligence Sharing and Release Policy in September 2013, the equivalent policy was to be found in "Reporting Policy – Sensitive Professions" (see [CM2-5]) which applied between December 2010 and September 2013 and in Reponses 27 and 28 (see [CM2-6]) which applied between 2005 and December 2010. The changes to the policy on the interception and reporting of legally privileged communications in the first half of 2015 brought with it a lowering of the threshold for sensi-check for the reporting of privileged material. Presently, all reporting that mentions a lawyer must be submitted to sensi-checkers, who will refer a high number of these reports to Legal Advisers. Formerly, only reporting on the communications of a lawyer went via this route. As a result of the implementation of the 2015 policy and process amendments, the amount of reporting referred by sensi-checkers to Legal Advisers to ascertain whether or not the contents of an intelligence report carries legal privilege or not has arisen.
- 16) The "Sensi-Checking: How To Guide" (see [CM2-7]), contains a separate section on legal privilege. This makes clear that reporters and reporting quality checkers are not qualified or permitted to decide whether:
 - a) the communications are privileged – this is reserved to Legal Advisers (LA) or to sensi-checkers or

- b) reporting the privileged communications is necessary and proportionate – this is reserved to sensi-checkers (acting on legal advice if appropriate).
- 17) Further it is made clear that the act of sensi-checking any such reporting is not sufficient to meet the Code of Conduct and it is vital that the additional consideration required is given and recorded. This is followed by a step by step guide to identifying whether the material is privileged which is used by sensi-checkers; guidance on the sending of reports to Legal Advisers; guidance on the reporting of such material including whether caveats should be added to the report and guidance on sensi-check exceptions (where the subject happens to be a lawyer but where the information obtained from them is routinely not privileged). The current version of the "Sensi-Checking: How To Guide" is dated March 2015 and the previous version of that Guide was last updated in December 2013.
- 18) Legally privileged material is not shown to lawyers engaged in relevant litigation. The practice underpinning this, known as Information Barriers, is set out in [CM2-8]. It is awaiting formal approval by the relevant GCHQ senior official. However, this policy has been followed in practice across the department since the Belhaj ruling, and reflects longstanding practice before that date.
- 19) As of June 2015, the Review and Retention section of the Compliance Guide states that material that contains legally privileged or other confidential information, or directly involves British Parliamentarians, and that is not required for intelligence reporting purposes must be deleted as soon as practicable, and that requests for exceptional retention of such material are unlikely to be approved. Following the Belhaj ruling, GCHQ made changes to the arrangements for the retention of legally privileged material. Prior to the Belhaj claim, non-reissued intelligence reports were retained in GCHQ's intelligence report repository along with all other intelligence reports. Following Belhaj, GCHQ has taken steps to ensure the isolation of any legally privileged intelligence reports which have been retained in the repository and do not meet the threshold for onward reporting by GCHQ to its customers. GCHQ now intends to institute routine isolation and deletion on a rolling basis; intelligence reports will continue to exist in the intelligence report repository for six months in order to give all relevant analysts the opportunity to assess the relevance of the intelligence. After this time non-reissued legally privileged intelligence reports will be moved into isolation and will become subject to strict access controls. These isolated intelligence reports will be routinely deleted on a rolling monthly basis.
- 20) I also attach (see [CM2-9]) an up-to-date summary of GCHQ's policy and guidance in relation to the special protection afforded to legally privileged information and other especially sensitive communications.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed: 

Dated: 23 November 2015

Statement No 3
For the Respondents
Dated 24 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/14/85/CH

PRIVACY INTERNATIONAL

Claimant

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/120-126/CH

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

THIRD WITNESS STATEMENT OF CIARAN MARTIN

I, **Ciaran Liam Martin**, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

- 1) I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also

have wider responsibilities for GCHQ's external communications and policy. I have been in this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

- 2) This is my third witness statement in these proceedings which I am authorised to make on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.
- 3) In this third statement I respond to certain statements in the Claimants' evidence.

Claimants' evidence

Professor Anderson

- 4) At §§21-23 of Professor Anderson's evidence he asserts that the intrusion which occurs during CNE activities "may place lives at risk" and he cites an example of political opponents hacking servers in hospitals in Oregon which interfered with medical equipment and put lives at risk.
- 5) GCHQ's CNE activities are carefully monitored, planned, authorised and inspected. We can only use any of our capabilities when it is necessary and proportionate to do so. So, whilst CNE, like a very broad range of other human activity, can put lives at risk if conducted in a reckless and irresponsible way, putting the lives of innocent members of the public at risk is not acceptable to GCHQ. GCHQ never carries out reckless and irresponsible CNE operations. That would be unlawful and we do not do it.
- 6) Additionally, GCHQ's processes for CNE include an expert risk assessment panel. This is referred to in my first statement at §65.

Eric King

- 7) In terms of the scale of CNE operations (see §§136-141 of Mr King's statement), GCHQ cannot confirm or deny assertions regarding the scale of its operations. However, it is simply not correct to assert that GCHQ is using CNE on an indiscriminate and disproportionate scale. As discussed at §28 of my first statement, CNE is a critical GCHQ tool.

Professor Sommer

- 8) I would not accept Professor Sommer's criticism of the CNE Code on the basis that the type of activity which is involved is too imprecise (see §11ff of his statement). The definitions in §1.6 of the Code do broadly reflect the type of CNE which is conducted and it is to be noted that the Ministerial Foreword to the Consultation Document published with the Code also gave further detail including that it applies to different investigative techniques (i.e. different from interception) including "the use of computer network exploitation, to identify, track and disrupt the most sophisticated targets."
- 9) Nor would I accept his statement about the role of Ministers. Professor Sommer asserts that politicians have an insufficient understanding of the methods which are employed, e.g. by GCHQ, in the CNE field, such that they are unable properly to assess necessity and proportionality when authorising warrants/authorisations under s.5 and s.7 ISA.
- 10) It is our responsibility within GCHQ to make sure that we explain the nature of our proposed activity and the intelligence requirements for it so that those who have to authorise the activity can do so on a fully informed basis. It is for that reason that we provide detailed information in support of the s.5 and s.7 warrants/authorisations, as required under the CNE Code. In terms of the CNE Code, it is to be noted that following the public consultation process, the Equipment Interference Code of Practice was laid before Parliament on 4 November 2015. However the paragraphs and paragraph numbers referred to in this and my previous statement are unaltered.
- 11) This detailed information is then given serious attention by senior Ministers and their advisers. In respect of s.5 and s.7 warrants/authorisations, the FCO has a unit headed at Director General level which, inter alia, advises the Foreign Secretary on authorisation applications. Part of this process involves seeking advice from the department's lawyers, whose views are reflected directly. Meetings to discuss individual warrants/authorisations, and/or requests for further information, and/or requests for different options, are common. As such, Ministers engage very significantly in the detail of the authorisations process and scrutinise carefully the methods that are employed.
- 12) As to the issues raised at §§96.2 and 108-111 of Professor Sommer's statement, there are precautions which are applied where there is any risk that CNE activities may have the potential to affect evidence in future criminal prosecutions.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed: *Clare M. Ki*

Dated: *24 November* 2015

Statement No 3
For the Respondents
Dated 24 November 2015

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/14/85/CH

PRIVACY INTERNATIONAL

Claimant

-and-

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS
- (2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

Case No. IPT/120-126/CH

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

-and-

- (1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS
- (2) GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

THIRD WITNESS STATEMENT OF CIARAN MARTIN

I, Ciaran Liam Martin, of Government Communications Headquarters (GCHQ), Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, WILL SAY as follows:

- 1) I am the Director General for Cyber Security at GCHQ and a member of GCHQ's main Board. In that role, I am responsible for GCHQ's statutory responsibilities for information security in the United Kingdom and its work protecting the UK from cyber threats. I also

have wider responsibilities for GCHQ's external communications and policy. I have been in this role since February 2014, having previously served in the Cabinet Office as Director of Constitutional Policy, Director of Security and Intelligence, and head of the Cabinet Secretary's Office. I have been a public official since 1997.

- 2) This is my third witness statement in these proceedings which I am authorised to make on behalf of the Respondents. The contents of this statement are within my own knowledge and are true to the best of my knowledge and belief. Where matters are not within my own knowledge they are based upon documentation made available to me and from discussions with others within the department.
- 3) In this third statement I respond to certain statements in the Claimants' evidence.

Claimants' evidence

Professor Anderson

- 4) At §§21-23 of Professor Anderson's evidence he asserts that the intrusion which occurs during CNE activities "may place lives at risk" and he cites an example of political opponents hacking servers in hospitals in Oregon which interfered with medical equipment and put lives at risk.
- 5) GCHQ's CNE activities are carefully monitored, planned, authorised and inspected. We can only use any of our capabilities when it is necessary and proportionate to do so. So, whilst CNE, like a very broad range of other human activity, can put lives at risk if conducted in a reckless and irresponsible way, putting the lives of innocent members of the public at risk is not acceptable to GCHQ. GCHQ never carries out reckless and irresponsible CNE operations. That would be unlawful and we do not do it.
- 6) Additionally, GCHQ's processes for CNE include an expert risk assessment panel. This is referred to in my first statement at §65.

Eric King

- 7) In terms of the scale of CNE operations (see §§136-141 of Mr King's statement), GCHQ cannot confirm or deny assertions regarding the scale of its operations. However, it is simply not correct to assert that GCHQ is using CNE on an indiscriminate and disproportionate scale. As discussed at §28 of my first statement, CNE is a critical GCHQ tool.

Professor Sommer

- 8) I would not accept Professor Sommer's criticism of the CNE Code on the basis that the type of activity which is involved is too imprecise (see §11ff of his statement). The definitions in §1.6 of the Code do broadly reflect the type of CNE which is conducted and it is to be noted that the Ministerial Foreword to the Consultation Document published with the Code also gave further detail including that it applies to different investigative techniques (i.e. different from interception) including "the use of computer network exploitation, to identify, track and disrupt the most sophisticated targets."
- 9) Nor would I accept his statement about the role of Ministers. Professor Sommer asserts that politicians have an insufficient understanding of the methods which are employed, e.g. by GCHQ, in the CNE field, such that they are unable properly to assess necessity and proportionality when authorising warrants/authorisations under s.5 and s.7 ISA.
- 10) It is our responsibility within GCHQ to make sure that we explain the nature of our proposed activity and the intelligence requirements for it so that those who have to authorise the activity can do so on a fully informed basis. It is for that reason that we provide detailed information in support of the s.5 and s.7 warrants/authorisations, as required under the CNE Code. In terms of the CNE Code, it is to be noted that following the public consultation process, the Equipment Interference Code of Practice was laid before Parliament on 4 November 2015. However the paragraphs and paragraph numbers referred to in this and my previous statement are unaltered.
- 11) This detailed information is then given serious attention by senior Ministers and their advisers. In respect of s.5 and s.7 warrants/authorisations, the FCO has a unit headed at Director General level which, inter alia, advises the Foreign Secretary on authorisation applications. Part of this process involves seeking advice from the department's lawyers, whose views are reflected directly. Meetings to discuss individual warrants/authorisations, and/or requests for further information, and/or requests for different options, are common. As such, Ministers engage very significantly in the detail of the authorisations process and scrutinise carefully the methods that are employed.
- 12) As to the issues raised at §§96.2 and 108-111 of Professor Sommer's statement, there are precautions which are applied where there is any risk that CNE activities may have the potential to affect evidence in future criminal prosecutions.

Statement of Truth

I believe that the facts stated in this statement are true.

Signed: *Ernie M. Ho*

Dated: *24 November* 2015

BETWEEN:

PRIVACY INTERNATIONAL
GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC.
CHAOS COMPUTER CLUB

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Defendants

SKELETON ARGUMENT SERVED ON
BEHALF OF THE CLAIMANTS

For hearing: Tuesday 1 December 2015

References in the form [AX/Y] are to Volume X, Tab Y of the Authorities Bundle.

References in the form [BX/Y/Z] are to Tab X, Page Y, Paragraph Z of the Open Bundle.

References beginning "CM" are to exhibits to the witness statements of Ciaran Martin.

References in the form [DX/Y/Z] are to Tab X, Page Y, Paragraph Z of the Open Documents.

A. Introduction

1. This case is about whether GCHQ has complied with domestic law and the ECHR when carrying out computer hacking¹ and deploying malware².
2. Until the open response was served, GCHQ refused to confirm or deny whether it had CNE capabilities, or had ever used them. This was a bizarre stance, since computer hacking tools are freely commercially available³, and regularly used. As Professor Sommer put it "*if certain exploit tools can be deployed by 16 and 17 year olds to significant effect... then it would be very surprising if GCHQ were not able to call upon and use similar or better techniques*" [BB/69/17]. A more sensible approach is now taken; GCHQ has co-

¹ Known within the Agencies as CNE, Computer and Network Exploitation.

² A portmanteau word: malicious software, designed to intrude or have other effects unwanted by the owner or user of the computer.

³ See [DA/99] ('Hacking Team', a commercial provider of CNE) and [69/15] (Report, Sommer).

operated in the production of a detailed schedule of avowals. With the possible exception of 'bulk CNE' (Issue 6(e))⁴, the schedule has been agreed.

3. Further, until this claim was brought, GCHQ's CNE operations had been conducted without public knowledge of the applicable safeguards. The consequences have been predictable. When rules governing surveillance are not subject to public scrutiny or testing, public authorities tend to interpret their legal powers to maximise their ability to use intrusive measures, whilst failing to put in place adequate safeguards. As in other recent cases, litigation has spurred a belated attempt at compliance with the law.

CNE

4. Strong safeguards governing CNE are needed because, when deployed against an individual's computer or telephone, CNE can achieve results that are at least as intrusive as if the targeted individual were to have his house bugged, his home searched, his communications intercepted and a tracking device fitted to his person.
5. The intrusiveness of gaining access to a modern telephone was summarised by Chief Justice Roberts in *Riley v California* in the Supreme Court of the United States. The basic point is that "a cell phone search would typically expose to the government far more than the most exhaustive search of a house..." As Roberts CJ explained:

"Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video — that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier..."

6. Further, CNE techniques can be deployed against entire networks of communications infrastructure, giving access to numerous computers at once. The consequence is the ability to gain bulk access to the data of very large numbers of people.

⁴ It is not understood why GCHQ is not willing to avow Bulk CNE, given that it told David Anderson QC it needed "the continued ability to acquire bulk data from a variety of sources, including through the use of new techniques, such as CNE" [CM1/7/258/10.40(a)]. Whether or not that means as a matter of strict construction that Bulk CNE is currently taking place, there can no longer be any serious prospect of any harm to national security from such confirmation being given, and the Respondents have made no effort to explain why they think there might be.

7. CNE is not a passive means of collecting intelligence, in contrast to interception. It requires active intrusion into a persons' computer, and often involves changing and altering the system to serve the purpose of the intruder. This has important consequences for the quality of the legal regime needed.
8. An intrusion into property that is not merely passive (such as a section 8(1) or 8(4) RIPA intercept) requires the strongest safeguards, not least because evidence obtained by CNE (and computers subject to CNE) is admissible in evidence, and forms the mainstay of many serious crime prosecutions. At its most serious, CNE can be destructive of people and property: for example, the 'Stuxnet' CNE operation which was aimed at disrupting nuclear centrifuges [BB/87/§72, DC/30].
9. Further, in order to carry out CNE, GCHQ must either seek or induce security holes in the systems that protect our computers, telephones and networks. Some of the more troubling elements of the Snowden disclosures are that the Five Eyes agencies have engaged in activities that weaken computer security for all (see Professor Anderson at [BB/54/§§49-77] and Mr King at [BB/22/§§70-116]). This has created a market in buying and selling computer vulnerabilities to nation states, and a strong incentive for nation states to weaken computer security to facilitate their access (see Professor Anderson at [BB/50/§§33-48] and Mr King at [BB/24/§§78-80]). Further, like any complex computer software, malware may have serious unintended effects. At the simplest level, users may be left vulnerable. Malware may spread beyond the intended targets.

Principles

10. CNE is thus a powerful and flexible technique, which carries greater risks to privacy and the security of the community than other forms of surveillance. In some limited cases, its covert use to gather information may be necessary and proportionate, subject to proper safeguards. Some CNE operations represent "... a reasonable extension of how civilised societies have dealt with law enforcement intrusion into physical property for many years" [Professor Anderson BB/47/19].
11. The issue is the presence of proper safeguards. As David Anderson QC notes, echoing the language of the ECtHR case law:

"13.5 ... in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency: not just fashionable buzz-words, but the necessary foundation for the trust between government and governed upon which the existence of coercive and intrusive powers depends in a modern democracy". [CM1/7/304]

In consequence:

"13.18... if the acceptable use of vast state powers is to be guaranteed, it cannot simply be by reference to the probity of its servants, the ingenuity of its enemies or current technical limitations on what it can do. Firm limits must also be written into law: not merely safeguards, but red lines that may not be crossed" [CM1/7/307].

B. Issues

12. The parties have agreed preliminary issues of law as follows:

- a) **Issue 1: Computer Misuse Act 1990 ("CMA 1990").** Before the CMA 1990 was amended with effect from 3 May 2015:
 - i. Was an act contrary to section 3 CMA 1990 (essentially, an unauthorised act in relation to a computer with the intention of, or recklessness as to, impairing its operation) capable of being rendered lawful by a statutory warrant?
 - ii. Would CNE activities of a Crown servant in the course of his employment, if committed in a foreign country or against assets or individuals located in a foreign country, have amounted to an offence under section 3 CMA 1990 as though the activities had been committed in England and against assets or individuals located in England?
- b) **Issue 2: 'Thematic' warrants under section 5 Intelligence Services Act 1994 ("ISA 1994").** Does section 5 ISA 1994 permit the issue of a 'thematic' warrant authorising acts in respect of a class of property, or must such a warrant specifically identify the property to which it relates?
- c) **Issue 3: Meaning of "property" in section 5 ISA 1994.** Does the power in section 5 ISA 1994 to issue a warrant authorising interference with "*property*" permit the issue of a warrant authorising interference with intangible legal rights, such as copyright or contractual rights?
- d) **Issues 4 to 6: "In accordance with law"/"prescribed by law".** In view of the intrusiveness of CNE, has the regime governing CNE complied with Articles 8 and 10 of the European Convention on Human Rights at all times since 1 August 2009? In particular:
 - i) Is the regime sufficiently **foreseeable** in its operation?
 - ii) Are there sufficient safeguards to protect against **arbitrary conduct**?
 - iii) Is the regime **proportionate**?
 - iv) If domestic law permits the issue of 'class' or 'thematic' warrants, does that regime comply with the above requirements or is specific authorisation necessary?
 - v) What **records** ought to be kept and with what degree of specificity as to the activity and the justification for it?
 - vi) What safeguards are necessary to prevent the obtaining, storing, analysis or use of **legally privileged material** and other sensitive **confidential documents**?

- vii) What is the relevance of (i) the **various safeguards** relied upon by the Respondents, or (ii) the fact that until February 2015 it was **neither confirmed nor denied** that the Respondents carried out CNE activities at all?

C. Facts

13. Many of the relevant facts are now admitted. It is common ground that:
- a) GCHQ undertakes CNE operations both within the UK and overseas.
 - b) GCHQ undertakes both “*persistent*” CNE operations (where an implant “*resides*” on a computer for an extended period) and “*non-persistent*” operations.
 - c) The Agencies’ CNE activities include operations against specific devices, computer networks and other targets.
 - d) GCHQ has obtained warrants to authorise CNE under both section 5 and section 7 ISA 1994.
 - e) GCHQ had five class authorisations under section 7 in 2014.
 - f) In 2013, about 20% of GCHQ’s intelligence reports contained information derived from CNE.
14. In addition:
- a) **First**, the amount of information that can be derived through CNE techniques is large, and the nature of that information can be extremely sensitive. While interception of communications will result in the acquisition of information which an individual has chosen to communicate over a network, CNE may obtain information that a user has chosen not to communicate, for instance:
 - i) photos or videos stored on the device;
 - ii) documents;
 - iii) address book;
 - iv) location, age, gender, marital status, finances, ethnicity, sexual orientation, education and family; and
 - v) information collected through activation of the device’s microphone or camera without the user’s consent.
 - b) David Anderson QC refers to Snowden documents explaining several of these capabilities used by GCHQ: “*a programme called NOSEY SMURF which involved implanting malware to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, TRACKER SMURF which had the*

capability to provide the location of a target's smart phone with high-precision, and PARANOID SMURF which ensured malware remained hidden." [CM1/7/390/§15].

- c) **Second**, CNE involves an active intrusion into a device or network. CNE techniques are not limited to the acquisition of information; it can be used to amend, add, modify or delete information, or to instruct the device to act or respond differently to commands.
- d) **Third**, CNE allows for intrusion on a large scale. As well as specific devices, CNE can be used against networks of computers, or network infrastructure such as websites or internet service providers. For example, it appears that the Respondents carried out a CNE operation against a manufacturer of mobile phone SIM cards in order to allow the circumvention of its encryption and to enable "*harvesting... at scale*" [BB/18/§55].
- e) Other examples include a CNE operation giving access to "*almost any user of the Internet*" in a targeted country [BB/14/§40] and systems designed for "*industrial scale exploitation*", appropriating the processing power of the target's computers to carry out searches and bulk analysis work [King BB/14/§42, 41/§138].
- f) CNE can also be used against software, altering widely-used programs. For example, it appears that GCHQ has sought to modify or reverse-engineer commercially available software such as anti-virus software [DC/51/§4].
- g) **Fourth**, CNE may leave users vulnerable to further damage:
 - i) Malware installed on a device can be used by third parties with similarly intrusive effects or worse.
 - ii) The process necessary to install the malware without alerting the user or his security software may result in or preserve security vulnerabilities that could be exploited by third parties.
 - iii) If the CNE takes place on a large scale - for instance in relation to network infrastructure, software, or common security protocols - it weakens security for all users, increasing the risk of exploitation by a third party. [Anderson BB/53/§§49-77].

D. Legislative framework

15. The legislative framework is set out in Annex 1 below.

E. Submissions

Issue 1a - section 10 of the CMA 1990

16. Many CNE operations will fall within section 3 CMA 1990. While a simple theft and use of login credentials would probably only engage section 1, section 3 could be engaged by:

- a) the bypassing of security protections, particularly if those protections are weakened even temporarily as a result;
 - b) the use of the microphone or camera on a device in such a way as to drain the battery or slow the device down;
 - c) the processing or exfiltration of data, if to do so involves a significant use of system resources or bandwidth; or
 - d) the weakening of encryption or security protocols operated by the computer.
17. On a proper construction of section 10 CMA 1990, prior to amendment in May 2015:
- a) a warrant (whether under ISA 1994 or PA 1997) could authorise CNE that would be a breach of section 1 CMA 1990 (i.e. hacking into a computer) but,
 - b) a warrant could not authorise CNE that would amount to the more serious offence of a breach of section 3 CMA 1990 (i.e. hacking into a computer and impairing its operation, including temporarily).
18. Parliament permitted law enforcement and intelligence agencies to gain access to computers to obtain information, but within strict limits. What Parliament did not authorise was CNE that impairs the operation of a computer.
19. Section 10 CMA 1990, prior to its amendment, provided: "*Section 1(1) above has effect without prejudice to the operation ... in England and Wales of any enactment relating to powers of inspection, search or seizure*". The corollary is that section 3 does not have effect without prejudice to such enactments; Parliament placed limits on interference with computers. Section 5 ISA 1994 (and the equivalent provisions of PA 1997) are plainly enactments "*relating to powers of inspection, search or seizure*". They permit the electronic inspection and search of a computer.
20. Where a statute expressly provides for consequences only in one class of case, it follows that those consequences are excluded for other classes of case which could have been identified but were not.
21. There are sound reasons why Parliament set these limits:
- a) First, the privacy intrusion involved in a section 1 offence more closely resembles a traditional search of premises or property. The section 3 offence is different: this type of hacking actually impairs the targeted device.
 - b) Secondly, the product of CNE is admissible in evidence. In that respect it is different from intercept evidence, which is inadmissible by section 17 RIPA 2000 and was inadmissible at the time of the passage of CMA 1990 under equivalent provisions of the Interception of Communications Act 1985. If state authorities are permitted to alter or impair the operation of a computer, the reliability and admissibility of such evidence will be called into question, as will the need to disclose a past CNE operation to the defence.

- c) Thirdly, section 10 of CMA 1990 also applies to authorisations under PA 1997, as well as a section 5 ISA warrant. The above points apply with the same or greater force in relation to the police.
 - d) Finally, powers of search and seizure are to be construed narrowly against the public body seeking to search.
22. The same analysis also applies to authorisations under section 7 ISA.
23. The Snowden documents indicate that GCHQ's internal view was that section 10 of the CMA 1990 operated as set out above. A document prepared by a representative of GCHQ in September 2010 records a "concern" that a particular CNE technique which "causes modification to computer data and will impact the reliability of the data" "may be illegal", because "The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material." [BA/9/§18(b)]
24. The Respondents' arguments as to why conduct constituting a s.3 offence may nevertheless be authorised lack merit:
- a) It is irrelevant that ISA 1994 post-dates CMA 1990 (Open Response [BA/103/§146A(a)]). Section 5 ISA substantially re-enacts section 3 SSA 1989, which permitted the Secretary of State to issue a warrant "authorising the taking of such action as is specified in the warrant in respect of any property so specified". That provision pre-dated CMA 1990. When Parliament passed CMA 1990, it had already given the Security Service property interference powers, which were discussed in Parliament as permitting covert searches.
 - b) The ISA does not provide express authorisation for equipment interference. Section 5 is framed as a general power to authorise property interference. There are many types of property interference, or interference with electromagnetic emissions, that have nothing to do with a computer. For good reasons, the *lex specialis* in the CMA 1990 limits the scope of this broad power in the special case of interference with computers.
 - c) The Respondents argue at [BA/105/§146A(f)] that "The interpretation contended for by the Claimants would lead to the absurd result that the authorisation mechanisms in the ISA could have no legal effect unless there was an express savings provision in each relevant piece of legislation". That is incorrect. The point is not just that there was no savings provision in respect of the s.3 offence; it is that there was an express savings provision which could easily have applied to the s.3 offence but which instead applied only to the s.1 offence. That is a clear indication of Parliament's intention that there was to be no possibility of authorising a commission of the s.3 offence in pursuit of powers of inspection, search or seizure.

25. It is common ground that the Serious Crime Act 2015 has now altered the position. The amendments to section 10 are not retrospective, so the issue still arises for determination in respect of the period before 3 May 2015.

Issue 1b – Extraterritorial effect of CMA 1990

26. GCHQ now accept that CNE activities abroad will ordinarily breach CMA 1990 in the absence of authorisation (“*class authorisations signed by the Secretary of State under section 7 of the ISA... removes liability under the Computer Misuse Act 1990*”) [DD/5].
27. However, if this remains in dispute:
- a) The jurisdictional provisions in CMA 1990 require “*at least one significant link with domestic jurisdiction*” (section 4(2)).
 - b) There will be such a link if the accused was in “*the home country*” at the time when he did the act constituting the offence (section 5(2-3)).
 - c) The “*home country*” is England and Wales, Scotland or Northern Ireland as appropriate (section 4(6)).
 - d) GCHQ operates from sites in Cheltenham, Scarborough and Bude. Any CNE carried out from those locations over computers anywhere in the world will be subject to CMA 1990.
 - e) Further, since the 2015 Act has come into force, any conduct abroad by a UK national which satisfies a dual criminality requirement will also be a “*significant link with domestic jurisdiction*” (section 5(1A)).
 - f) In any event, section 31 of the Criminal Justice Act 1948 deems conduct carried out abroad by Crown servants acting or purporting to act in the course of their employment to be subject to English criminal law.

Issue 2 – ‘Thematic’ warrants under section 5 ISA

28. The issue of construction of section 5 ISA was accurately identified and properly brought to public attention by Sir Mark Waller in his 2014 Report, published on 25 June 2015⁵:

“ • Thematic Property Warrants

I have expressed concerns about the use of what might be termed “thematic” property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers “to a particular act” or to “acts” undertaken in the course of an operation. However, section 5 is narrower referring to “property so specified”.

⁵ A keen reader of the ISC report (published on 12 March 2015) might have spotted a passing reference to thematic property warrants in footnote 34 of Chapter 3, three months prior to Sir Mark’s report [CM14/581], but the Claimants did not.

During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or "thematic". I have expressed my view that:

- section 5 does not expressly allow for a class of authorisation; and
- the words "property so specified" might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals. The agencies and the warrantry units argue that ISA refers to action and properties which "are specified" which they interpret to mean "described by specification". Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which "specifies" property by reference to a described set of persons, only being able to identify with precision an individual at a later moment". [CM1/16/849]

29. Sir Mark Waller was unwilling to go further than to note that the Agencies' interpretation was "very arguable". He recorded that one of the agencies had withdrawn a 'thematic' property warrant in light of his views [CM1/16/849]. Sir Mark is only content for a 'thematic' warrant to be issued "where there is no intrusion into privacy" (Martin 1 §71H).
30. A warrant power should be strictly construed. However, the Respondents have interpreted section 5 in an exorbitant manner. The Respondent claims that "property so specified" in a section 5 warrant can instead be "specified... by description", as opposed to by identification of the specific property [BA/107/146D(a)(v)]. That cannot be correct. It would permit a section 5 warrant to authorise property interference/CNE in the UK over:
- a) "all mobile telephones in Birmingham";
 - b) "all computers used by suspected members of a drug gang";
 - c) "all copies of Microsoft Windows used by a person in the UK who is suspected of having travelled to Turkey in the last year"; or
 - d) "all software obtained by GCHQ".
31. The over-broad use of section 5 ISA is illustrated by some of the Snowden documents. On 22 June 2015, it was publicly disclosed that GCHQ had applied under section 5 ISA 1994 for a warrant authorising "all continuing activities which involve interference with copyright or licensed software" including "modifying commercially available software to enable interception, decryption and other related tasks or "reverse engineering" software" [DC/51-52/§1, 7].

32. The Agencies' expansive interpretation of section 5 ISA is wrong:

- a) First, it would collapse the distinction between a section 5 'warrant' and a section 7 'authorisation'. Section 7 permits an authorisation of "acts of a description" or "acts undertaken in the course of an operation so specified" or acts affecting "persons of a description so specified". It therefore expressly permits the general authorisation of an entire operation, or a class of conduct. GCHQ appears to have made great use of that power, conducting all of its foreign CNE and other foreign activities pursuant to only five class authorisations [CM1/13/645/§234]. No similar wording permitting the authorisation of such wide classes or thematic operations is present in section 5.
- b) Secondly, a 'thematic' warrant is in truth, a general warrant. A dislike of general warrants is a long-established principle of the common law. A 'thematic' warrant could only be available if clear words were used, thus overriding the limits long respected by the common law on the proper scope of state interference with property within the jurisdiction:
 - i) Under the principle of legality, Parliament is taken not to have interfered with fundamental rights, unless it uses clear words. See *R v SSHD, ex parte Simms* [2000] 2 AC 115 at 131 per Lord Hoffmann:

"Parliamentary sovereignty means that Parliament can, if it chooses, legislate contrary to fundamental principles of human rights. The Human Rights Act 1998 will not detract from this power. The constraints upon its exercise by Parliament are ultimately political, not legal. But the principle of legality means that Parliament must squarely confront what it is doing and accept the political cost. Fundamental rights cannot be overridden by general or ambiguous words. This is because there is too great a risk that the full implications of their unqualified meaning may have passed unnoticed in the democratic process. In the absence of express language or necessary implication to the contrary, the courts therefore presume that even the most general words were intended to be subject to the basic rights of the individual. In this way the courts of the United Kingdom, though acknowledging the sovereignty of Parliament, apply principles of constitutionality little different from those which exist in countries where the power of the legislature is expressly limited by a constitutional document."

- ii) A general warrant allows state officials, with no limits on time or place, to investigate a broad class of undesirable *conduct* (typically sedition in the 1700s, or a threat to national security now), rather than intrude on a specified *suspect* or *place*. In 1644, Coke condemned general warrants, as did Sir Matthew Hale in 1736. Hale explained that a "general warrant to search in all suspected places is not good" and "not justifiable" because it gave

such discretion to mere Crown servants "to be in effect the judge" (History of the Pleas of the Crown, p. 150).

- iii) Most of the leading common law property interference cases concern general warrants. In all the cases, the threat to national security was urgent, and necessity may have required a warrant covering an operation rather than specified property. But the common law did not accede:
 - a) In *Huckle v Money* (1763) 2 Wilson 205, 95 ER 768 Lord Pratt CJ noted that: "To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject".
 - b) In *Wilkes v Wood* (1763) Lofft 1, 98 ER 489 the Lord Chief Justice said: "The defendants claimed a right, under precedents, to force persons houses, break open escrutores, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject." See also *Entick v Carrington* (1765) 2 Wilson 275.
- iv) In the absence of clear and express words, Parliament has not departed from the traditional limits on search and seizure within the UK. There is nothing objectionable in a warrant that defines its target by reference to a specified person or premises. But legislation should not readily be construed as permitting a covert general warrant within the UK, in the absence of clear words, nor is such legislation necessary or proportionate.
- c) Finally, if section 5 is ambiguous (which it is not), reference to Hansard assists:
 - i) Sections 5(1) and 5(2) ISA are based on sections 3(1) and 3(2) of the Security Service Act 1989, which permitted the Secretary of State to issue a warrant "authorising the taking of such action as is specified in the warrant in respect of any property so specified". In promoting the Security Service Bill, John Patten MP, the Minister of State for Home Affairs, explained to Parliament that a warrant issued under this power could only authorise "action in respect of a named property, and both the action and the name of the property must be on the warrant" (HC Deb 17 January 1989 vol 145, col 269, underlining added).
 - ii) Equally, the Claimants have found nothing in the Parliamentary debates leading to the passing of the ISA to suggest that Parliament contemplated that a section 5 warrant could authorise interference with a class of

property, specified by a broad description, as opposed to a specified item of property.

Issue 3 – Intangible property

33. The power in section 5 ISA permits interference with real property and personal property. It does not permit interference with a chose in action, such as intellectual property (or any other intangible right).⁶
34. The meaning of the word “property” depends on the context in which it is used.
- a) In *R v Khan (Sultan Ashraf)* [1982] 1 WLR 1405, a deprivation order was made for the forfeiture of a convicted heroin dealer’s house. The relevant power was contained in section 43(1) Powers of Criminal Courts Act 1973, which empowered a court to make an order in respect of “property which was in his possession or under his control at the time of his apprehension” which “has been used for the purpose of committing, or facilitating the commission of, any offence”. The Court of Appeal overturned the order on the grounds that the section was confined to “personal property and not real property”. Per Dunn LJ at 1408: “subsection (4), which makes the Police Property Act 1897 applicable, refers to property which is in the possession of the police by virtue of the section, thus confining it to personal property and not real property.”
 - b) In *Welsh Development Agency v Export Finance Co Ltd* [1992] BCC 270, the Court of Appeal held that section 234 Insolvency Act 1986, in protecting an office-holder in certain circumstances where he “seizes or disposes of any property which is not property of the company”, was limited to tangible property. Per Dillon LJ at 287: “But subsec. (3) and (4) repeat the word ‘seized’ which was used in sec. 61 and is in its natural sense only applicable to tangible property and not to choses in action. Beyond that, se. 234(2) enables the court to give relief ‘Where any person has in his possession or control any property, books, papers or records to which the company appears to be entitled’; that again appears at least primarily to be dealing with tangible property only. In my judgment, the references in sec. 234(3) and (4) to seizing property only apply to tangible property, and do not apply to choses in action.”
35. The provisions of ISA 1994 contain several clear indications that section 5 is concerned only with interference with physical property:
- a) Section 5(3) and (3A) impose restrictions in relation to the issue of warrants in respect of “property in the British Islands”.
 - b) Section 7(10) provides:
 - “Where-
 - (a) A person is authorised by virtue of this section to do an act outside the British Islands in relation to property;

⁶ One of the Snowden documents indicates that “the Intelligence Services Commissioner was consulted in 2005 on the applicability of a warrant in these circumstances [in relation to intellectual property as embodied in copyright or licensing agreements] and he was content that section 5 could be used to remove such liability” [DC/54/§17].

- (b) The act is one which, in relation to property within the British Islands, is capable of being authorised by a warrant under section 5;
 - (c) A person authorised by virtue of this section to do that act outside the British Islands, does the act in relation to that property while it is within the British Islands, and
 - (d) The act is done in circumstances falling within subsection (11) and (12)."
- c) Section 7(11) provides: "An act is done in circumstances falling within this subsection if it is done in relation to the property at a time when it is believed to be outside the British Islands."
- d) Section 7(12) provides:
- "An act is done in circumstances falling within this subsection if it -*
- (a) *Is done in relation to property which was mistakenly believed to be outside the British Islands either when the authorisation under this section was given or at a subsequent time or which has been brought within the British Islands since the giving of the authorisation; but*
 - (b) *Is done before the end of the fifth working day after the day on which the presence of the property in the British Islands first becomes known."*
- e) Section 7(13) and (14) make further provision in relation to the relevant dates for the purposes of section 7(12), and refer to "the belief that the property was outside the British Islands", the property being "within those Islands", and the property being "brought within the British Islands".
36. These provisions are inconsistent with section 5 covering intangible property, such as a chose in action or a copyright. How can a copyright or right of action be "brought within the British Islands"?

Copyright

37. A particular issue arises in respect of interference with copyright, in view of the rights conferred by the Copyright Directive (Directive 2001/29).
38. Article 2 of Directive 2001/29 provides: "Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part (a) for authors, of their works ...".
39. National law must so far as possible be construed in accordance with that obligation, in accordance with the principle in Case C-106/98 Marleasing: ITV Broadcasting Ltd v TVCatchup Ltd [2011] EWHC 2977 (Pat) at [35].

40. Article 5 of the Directive sets out an exhaustive list of possible exceptions or limitations to the Article 2 right. The only relevant exception is Article 5.3(e), which enables Member States to provide for an exception for “*use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings*”. Further, Article 5.5 provides that such exceptions “*shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.*”
41. Accordingly, any interference with copyright by the authorities of a Member State must satisfy the following requirements of EU law:
- a) It must be clearly provided for in law, satisfying “*the need for legal certainty for authors with regard to the protection of their works*”: C-14/10 *Painer v Axel Springer* at [100-110];
 - b) It must not conflict with a normal exploitation of the work and must not unreasonably prejudice the legitimate interests of the rightholder: Article 5.5; and,
 - c) It must comply with the general EU law of proportionality, satisfying the “*relatively intensive and thorough*” standard of review which applies in respect of interferences with copyright: *BASCA v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin) at [135].
42. If the Respondents have been operating section 5 ISA 1994 so as to purport to justify interference with copyright for the purpose of reverse-engineering software, that is non-compliant with the first two requirements (and its compliance with the third is a question of fact). The reverse-engineering of software – presumably with a view to developing malware – obviously conflicts with the normal exploitation of those works.
43. In their pleaded Response, the Respondents say “*the relevance of Directive 2001/29 is not understood*” because “*the relevant law of copyright is the domestic law of England and Wales*” [BA/107/146F]. The Directive is relevant to the effect of domestic law for two reasons:
- a) First, because of the obligation recognised in *Marleasing* to interpret domestic legislation as far as possible in accordance with an EU directive. It is a heavy obligation: as Arden LJ held in *HMRC v IDT Card Services (Ireland) Ltd* [2006] EWCA Civ 29 at [82], in view of an inconsistent provision of EU law “*the English courts can adopt a construction [of domestic law] which is not the natural one.*” Even if Section 5 ISA were ambiguous (which it is not), *Marleasing* interpretation would require that it be construed in such a way as to preclude interference with copyright contrary to the Directive.
 - b) Second, because a Court is bound to give direct effect to “*unconditional and sufficiently precise*” provisions of a directive as against a public authority even if to do so would be *contrary* to domestic law: C-41/74 *Van Duyn v Home Office* at

[11]. Where rightholders are concerned, Article 2 of Directive 2001/29 is such a provision, and must therefore be given effect.⁷

Issue 4 - Prescribed by law

Foreseeability

44. By section 6 of the Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates the European Convention on Human Rights ("ECHR") [A1/6].
45. Article 8 of the Convention provides:
- "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
46. There are therefore four questions:
- a) Is the Article 8(1) right engaged?
 - b) Does the interference comply with the requirement of legal certainty imposed by the relevant Article?
 - c) Is the interference in pursuit of a legitimate aim?
 - d) Is the interference proportionate to the goal that is sought to be achieved (in the case of Article 8, "*necessary in a democratic society...*")? [A1/6]

Engagement of rights

47. Article 8 of the ECHR is clearly engaged in the present case.

Legal certainty

⁷ The Response also says, at [BA/107/146F]: "*It is not contended that the United Kingdom has failed to implement Directive 2001/29 in domestic law.*" It is unclear what is meant by that submission. As is clearly pleaded at [BA/22/41E], the Directive imposes certain requirements on a Member State. If those requirements have not been met – for instance because a public authority has interfered with copyright in a manner which does not meet them, or because the law is insufficiently clear as to whether there could be such an interference – then it follows the United Kingdom will have failed to implement Directive 2001/29 properly. In those circumstances the Court will have to give effect to it, either by reading down the domestic provisions, or giving effect to the Directive directly against a public authority in any case where a person's directly effective rights are engaged.

48. Any interference with Article 8 must be “in accordance with the law” (see Article 8(2) [A1/6]). This requires more than merely that the interference be lawful as a matter of English law: it must also be “compatible with the rule of law” (*Gillan v United Kingdom* (2010) 50 EHRR 45 at §76). There must be “a measure of legal protection against arbitrary interferences by public authorities”, and public rules must indicate “with sufficient clarity” the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.
49. There are therefore three sub-requirements:
- a) the conduct must comply with domestic law (legality);
 - b) the public rules must be sufficiently clear and describe the scope of any discretion and the manner of its exercise (foreseeability); and
 - c) there must be adequate legal protection against arbitrary interference with privacy (arbitrariness).
50. Numerous cases have addressed these requirements in the context of secret surveillance and information gathering:
- a) In *Malone v United Kingdom* (1985) 7 EHRR 14 [A2/42], the Court held that the legal regime governing interception of communications “must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence” §67. It must be clear “what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive” and the law must indicate “with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities” §79.
 - b) In *Association for European Integration and Human Rights v Bulgaria* (62540/00, 28 June 2007) [A2/30], the Court held at §75:

“In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated ...”
 - c) These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the “procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material” (*Liberty v UK* (2009) 48 EHRR 1 at §69).
 - d) In *Weber & Saravia v Germany* (2008) 46 EHRR SE5 [A2/49] the ECHR held at §§93-94:

“The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the

conditions on which public authorities are empowered to resort to any such measures ... Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

- e) In *Weber* the Court at §95 set out minimum safeguards (with numbers and spacing added for clarity):

"In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power:

[1] the nature of the offences which may give rise to an interception order;

[2] a definition of the categories of people liable to have their telephones tapped;

[3] a limit on the duration of telephone tapping;

[4] the procedure to be followed for examining, using and storing the data obtained;

[5] the precautions to be taken when communicating the data to other parties; and

[6] the circumstances in which recordings may or must be erased or the tapes destroyed."

- f) *Weber* was an interception case, but the principles in *Weber* have wider application to cases involving surveillance of all kinds. The touchstone is whether the degree of interference with privacy is comparable to that involved in interception of communication. See *RE v UK* at §130 ("the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference" [A2/44]. Cf. *Uzun v Germany* [A2/48] where the full *Weber* criteria were not applied because the case only involved collection of the location of a vehicle, generally on public roads or visible from the street. For the reasons set out above, CNE is at least as intrusive as traditional intercept, often far more so.

51. Applying these principles, the ECtHR has repeatedly held that the intercept and surveillance practices of the UK did not include sufficient public and binding safeguards and did not comply with the "in accordance with the law" requirement. See, for example, *Malone* [A2/42], *Liberty v UK* [A2/41], *Khan v UK* [A2/37] and *RE v UK* [A2/44].

Similarly, see *Liberty/Privacy* on foreseeability of 8(4) interception and *Belhaj* in the IPT (by concession) [A2/22-23 and A1/16].

52. This issue is not one in which the Court gives any margin of discretion to the state. See the judgment of Lord Reed in *R (T) v Chief Constable of Greater Manchester* [2014] 3 WLR 96 at §114:

“Whether a system provides adequate safeguards against arbitrary treatment, and is therefore “in accordance with the law” within the meaning of the Convention, is not a question of proportionality, and is therefore not a matter in relation to which the court allows national authorities a margin of appreciation.”

Domestic law

53. For the reasons set out above, GCHQ has not correctly understood or applied domestic law governing CNE. There is therefore a breach of the first limb of the “in accordance with the law” requirement.

Prior to the Open Response/First Draft EI Code

54. The *Privacy International* claim was issued on 13 May 2014. The Open Response was served on 6 February 2015, at the same time as the publication of the First Draft EI Code. Prior to the service of the Open Response, nothing at all was known about the rules or safeguards governing CNE. The *Weber* criteria were not satisfied:

- a) The Property Code was the only public information about the use of CNE (even assuming it could be deduced that property interference included CNE, which is far from obvious).
- b) The Property Code is very brief as applied to section 5 authorisations and does not engage with *Weber* requirements 4, 5 or 6.
- c) The position in relation to section 7 ISA is even worse. There was no Code of Practice governing the use of section 7 (nor even a power to issue one). Section 7 was an unexplained bare power, even though section 7 might often affect people in the United Kingdom. This may occur in three ways:
 - i) First, where a mistake is made as to location, or in the 5-day grace period under section 7(11) ISA.
 - ii) Secondly, where a person in the UK stores (as we all do) their data outside the UK. See *Martin* 1 at [BB/133/§44].
 - iii) Thirdly, foreign CNE conduct will often affect people in the UK. For example, if a CNE operation steals the keys for all SIM cards produced by a foreign manufacturer (such as Gemalto), many of those cards will end up in the UK and be used by UK persons.

The availability of a warrant that simply cancels any unlawfulness is self-evidently not an adequate safeguard against arbitrary conduct.

55. This absence of proper public procedures was not for good reasons of national security – the use of CNE was admitted once the claim had been brought, and was formally avowed in the ISC and Anderson Reports. The position is worse than the pre-IOCA 1985 days of intercept considered by the ECtHR in *Malone*. A useful comparator is *Liberty v UK* where there was no Code of Practice governing bulk interception under IOCA 1985, nor any public safeguards or limits on a wide statutory power. The subsequent introduction of the RIPA Interception Code of Practice demonstrated the inadequacy of what went before [A2/41].

56. The failing is not simply technical. As David Anderson QC puts it:

“Obscure laws – and there are few more impenetrable than RIPA and its satellites – corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean. Thus:

(a)... ISA 1994 ss 5 and 7... are so baldly stated as to tell the citizen little about how they are liable to be used” [CM1/7/310/§13.31].

After the Open Response/First and Second Drafts of the EI Code

57. Publication of the draft EI Code does not cure the problems:

- a) First, the specific failings in relation to the Draft EI Codes are set out below under issue 5.
- b) Secondly, the EI Code is only in draft, not yet approved.

Article 10 ECHR

58. The same analysis of the issues applies under Article 10 ECHR.

Issue 5

59. (a) *Specific and individual or class warrants:*

- a) The over-broad approach to the use of section 5 ISA thematic warrants has been considered above. The dangers of general warrants are present more strongly in the case of section 7 ISA class authorisations. There were only five such authorisations in place in 2014 which covered all of the agencies’ CNE activities abroad. All authorisation is then conducted internally. This absence of any meaningful external or independent approval for highly intrusive conduct is a significant failing in the regime. Several additional failures are set out below.
- b) First, under the draft EI Code there is inadequate protection for people in the British Islands whose data is obtained by CNE abroad. For example, assume a Londoner’s smartphone stores photographs on a computer server in the Republic of Ireland. GCHQ wishes to look at the photos. There are three sets of statutory powers it could use:

- i) Section 5 ISA could be used to obtain the photos directly from the smartphone using CNE. This would require a Secretary of State warrant.
- ii) RIPA could be used to obtain the photos. Interception under RIPA includes any time when information is stored after being transmitted (section 2(7) [A10]).
 - a) If section 8(1) of RIPA is used, a Secretary of State warrant would be required.
 - b) Assuming that a bulk warrant under section 8(4) of RIPA is used, the person has the equivalent safeguard that GCHQ would require a section 16(3) certification, which is for practical purposes identical to a Secretary of State warrant.
- iii) Section 7 ISA could be used to obtain the photos under GCHQ's class authorisation. No Secretary of State warrant is required, nor is there any equivalent certification procedure. GCHQ can authorise the obtaining of the photos internally. Important safeguards that are a crucial part of maintaining the lawfulness of the RIPA interception regime are absent.
- iv) In this scenario, the Draft EI Codes do not provide any substantial safeguard:

"If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7."

David Anderson QC rightly observes that the Code "*does not elaborate on what factors should be taken into account in the course of that consideration*" [CM7/161/6.33]. In contrast, other provisions of the Draft EI Codes are phrased in terms of "*should*" or "*must*".

- c) The important safeguard in RIPA of a Secretary of State warrant is thus liable to be circumvented by a general power in section 7. The protection given to the citizen is greatly reduced.
- d) Secondly, there are no procedures in the Draft EI Code requiring the use of filtering techniques where bulk CNE is carried out⁶ (see Issue 6(e) - "*the use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest*"). The Commissioner has encouraged the use of such filters when considering data collected under

⁶ The Claimants reserve their position as to the IPT's approach of the use of bulk collection in *Liberty/Privacy*.

section 7 ("I stressed to [GCHQ] the importance I place on filters which help avoid any unnecessary intrusion" [CM16/856]).

- e) However, the Commissioner's exhortation is not backed by any obligation, either in statute or a Code of Practice. Again, the contrast with RIPA is striking:
 - i) Under section 16(1) RIPA, inspection of bulk material is limited by a certificate. This is the key safeguard in respect of bulk collection. In *Liberty/Privacy* the Tribunal accepted Liberty's submission that section 16 was needed to do the "heavy lifting" of protecting privacy if a large volume of data was being collected. The Tribunal held "we do not accept that it is, simply, as Mr Eadie put it in Reply submissions, "procedural" [A2/22/§103].
 - ii) The certificate is supplemented by detailed provisions in the Interception Code of Practice requiring the use of automated filtering systems using an effective selection methodology, the giving of reasons before making any selection etc. These safeguards are essential to the lawfulness of such bulk techniques. They are not required in respect of material collected in bulk under section 7 ISA, either by the legislation, or the applicable Code of Practice (Section 7 of the Interception of Communications Code of Practice).
 - f) Finally, even where a section 5 ISA warrant is obtained, it could be used to target computer networks, servers and other devices used by individuals or organisations that are not of any intelligence interest in and of themselves.
60. (b) *Record keeping* - GCHQ contend that they keep better records than the other Agencies. This may be right (see Commissioner's 2014 report [CM1/17/856]). However, the records that are required to be kept by the draft EI Code are at the stage of authorising the CNE operation, not the documentation of the searches that take place of the data obtained.
61. (c) *Legal Professional Privilege* - The regime prior to the publication of the Draft EI Codes was not in accordance with the law for the same reasons as in *Belhaj*:
- a) GCHQ conceded in *Belhaj* that its procedures in relation to intercept of privileged material were not lawful.
 - b) Although the Property Code was drafted in better terms than the Interception Code (see [CM1/16/777/§4.26]), that was not reflected in GCHQ's internal policies. The concession in *Belhaj* was rightly made:
 - i) The definition of privilege in GCHQ's procedures is inadequate - it ignores litigation privilege. See [CM2-5/§14-16].
 - ii) The guidance does not recognise that 'events', metadata and communications data may be privileged (as to which see below). See [CM2-5/§5].

- iii) GCHQ had no internal information barrier policies to deal with cases in which it was a party to actual or potential litigation. The information barrier procedures applied by GCHQ were inadequate, leading to a determination against GCHQ in respect of Mr Al-Saadi.

62. The regime after the publication of the draft EI Codes remains inadequate:

- a) The First Draft EI Code proposed a number of welcome improvements:
 - i) Privilege is properly defined, by reference to section 98 of the PA 1997 [CM1/15/714/§3.2]
 - ii) Proper information barriers “*must*” be put in place to ensure that lawyers and policy officials do not see privileged materials, with provision for applying to the Court in cases of doubt [CM1/15/716/§3.17].
- b) The Second Draft EI Code proposed certain further improvements:
 - i) Communications between lawyer and client and between a lawyer and another person for the purposes of litigation are presumed to be privileged unless the contrary is established (para. 3.4).
 - ii) Sensibly, given the past tendency of the Agencies to introduce internal glosses on necessary and proper information barriers, the Code expressly provides that “*For the avoidance of doubt, the guidance in paragraphs 3.1 to 3.18 takes precedence over any contrary content of an agency’s internal advice or guidance*”.
- c) But the Second Draft EI Code also worsens the language by changing the mandatory “*must*” to a discretionary “*should*” (e.g. para. 3.17). The protection of privilege ought to be mandatory.
- d) Further, both Draft EI Codes are silent on whether ‘events’ information or metadata can be privileged. However, it is clear from GCHQ’s current internal procedures at [CM2-9] that GCHQ continues to consider that privilege does not attach to the fact of a communication between lawyer and client or witness or expert:

“Reporters should also remember that the additional sensitivity attaches to the content of the communications, not to the fact of communication having taken place. Metadata only reports featuring lawyers do not require mandatory checking by the relevant team.”

- e) This approach is wrong in law. Metadata will often be subject to legal professional privilege without sight of the content. For example, the fact of a communication between a lawyer and a potential witness is itself privileged information and will be disclosed by the fact of the communication alone. Whether a lawyer or client has spoken to a particular witness or potential expert is often very sensitive privileged information, deserving of strict protection. The dates, times, place and parties to legally privileged communications are

information that is as privileged as the substance of the communication. See *Passmore on Privilege*, 3rd Ed para. 9-007 - 9-008. Just as journalists are entitled to protect their sources, a litigant (or criminal defendant) is entitled to consult an expert or speak to a witness without the opposing party knowing that fact. In such cases, GCHQ's policies currently apply no information barriers, nor any restriction on the wider distribution of such information to partner agencies or others in government. For a detailed analysis of the legal errors in this approach, the Claimants rely on the submissions of the Law Society in the *DRIPA* litigation, a copy of which is attached to this skeleton.

- f) Even today, GCHQ has not formally introduced the proper information barrier procedures required by *Belhaj*. The procedures are still "awaiting formal approval by the relevant GCHQ senior official" (Martin 2, §18). An *ad hoc* Chinese wall policy is not sufficient in law. See *Prince Jefri Bolkiah v KPMG* [1999] 2 AC 222 Lord Millett at p. 239:

"... In my opinion an effective Chinese wall needs to be an established part of the organisational structure of the firm, not created *ad hoc*..."

63. (d) *Previous NCND stance* - The Claimants' submissions are set out above.
64. (e) *Property Interference Code* - The Claimants' submissions are set out above. In short, the Property Interference Code does not even recognise the existence of CNE, still less put in place appropriate procedures to deal with intrusive CNE operations.
65. (f) *Draft EI Codes* - The Claimants' submissions are set out above.
66. (g) *Commissioner's oversight* - The Commissioner's oversight has in the past been ineffective. For example:
- a) The Commissioners all failed to identify the defects in the Agencies' procedures that led to the concession in *Belhaj*.
- b) No inspection had ever been made of the "Additions layer" which is "the layer at which individual targets are usually described" under section 7 ISA until April 2015 [BB/141/§71I]. Mr Martin's explanation of the Commissioner's recommendations following the inspection is Delphic ("The Commissioner recommended changes be made to ensure that each element is dealt with explicitly and at the earliest opportunity"). A comprehensible explanation ought to be disclosed.
- c) The Commissioner had not identified that "until recent years, renewal instruments for section 5 warrants had contained the minimum wording stipulated by ISA section 6" [BB/141/§71E]. This appears to mean that a renewal instrument simply said words to the effect of 'I renew warrant [number] for 6 months.' The Commissioner asked GCHQ to add a reminder to the Secretary of State of the statutory test.
67. (h) *Role of the Tribunal* - The Claimants reserve their position as to whether it is proper for the Tribunal to consider any closed material for the purpose of determining the

preliminary issues. To the extent that any EU law issues arise, the Claimants note that there is no domestic right of appeal against a decision of the Tribunal.

Is the regime proportionate?

68. For the reasons set out above, the regime governing CNE was not and remains disproportionate. Given the high potential level of intrusiveness, including over large numbers of innocent persons, there are inadequate safeguards and limitations.

F. Conclusion

69. The Tribunal is invited to answer the Preliminary Issues as set out above.

BEN JAFFEY

TOM CLEAVER

Blackstone Chambers

BHATT MURPHY

25 November 2015

Annex 1 - Legislative Framework

Computer Misuse Act 1990

1. The CMA 1990 provides for specific (and often extra-territorial) criminal liability for CNE. There are two key offences:
 - a) Section 1 provides an offence of unauthorised access to a computer.
 - b) Section 3 provides for the more serious offence of impairing the operation of a computer, even temporarily.
2. The Section 1 offence carries a maximum sentence of two years' imprisonment:

“(1) A person is guilty of an offence if—

 - (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;
 - (b) the access he intends to secure, or to enable to be secured, is unauthorised; and
 - (c) he knows at the time when he causes the computer to perform the function that that is the case”.
3. The Section 3 offence carries a maximum sentence of ten years' imprisonment:

“(1) A person is guilty of an offence if-

 - (a) he does any unauthorised act in relation to a computer;
 - (b) at the time when he does the act he knows that it is unauthorised; and
 - (c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act-

 - (a) to impair the operation of any computer;
 - (b) to prevent or hinder access to any program or data held in any computer;
 - (c) to impair the operation of any such program or the reliability of any such data; or
 - (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

- (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.
 - (4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-
 - (a) any particular computer;
 - (b) any particular program or data; or
 - (c) a program or data of any particular kind.
 - (5) In this section ...
 - (c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily."
4. Sections 4 and 5 make various provisions in relation to the territorial scope of both offences.
- a) Section 4(1) provides that, subject to the remainder of that section, it is immaterial *"whether any act or event proof of which is required for conviction of the offence occurred in the home country [England and Wales, Scotland or Northern Ireland as appropriate] concerned"*.
 - b) Section 4(2) requires *"at least one significant link with domestic jurisdiction"*.
 - c) Section 5(3) provides that there is such a link in relation to the section 3 offence if *"the accused was in the home country concerned at the time when he did the unauthorised act (or caused it to be done)"* or *"the unauthorised act was done in relation to a computer in the home country concerned"*.
 - d) Section 5(2) makes similar provision in relation to the section 1 offence.
5. Section 31 CJA 1948 provides:
- "Any British subject employed under His Majesty's Government in the United Kingdom in the service of the Crown who commits, in a foreign country, when acting or purporting to act in the course of his employment, any offence which, if committed in England, would be punishable on indictment, shall be guilty of an offence and subject to the same punishment as if the offence had been committed in England."*
6. Section 10 CMA 1990 contains saving provisions:
- a) Prior to 3 May 2015, section 10 provided: *"Section 1(1) above has effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure ..."*

- b) Following its amendment by the Serious Crime Act 2015, s.10 now provides: "Sections 1 to 3A have effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required" (amendments underlined).
7. The 'Explanatory Notes' to the Serious Crime Act 2015 did not flag any significant change in relation to section 10. Instead, they said at paragraph 139:
- "Section 10 of the 1990 Act contains a saving provision. It provides that the offence at section 1(1) of the 1990 Act has effect without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure; and in Scotland of any enactment or rule of law relating to powers of examination, search or seizure. The amendment to section 10 of the 1990 Act made by this section is a clarifying amendment. It is designed to remove any ambiguity over the interaction between the lawful exercise of powers (wherever exercised) conferred under or by virtue of any enactment (and in Scotland, rule of law) and the offence provisions. "Enactment" is expressly defined to provide certainty as to what this term includes. The title of section 10 of the 1990 Act has also been changed to remove the reference to "certain law enforcement powers" (see paragraph 12 of Schedule 4). This is to avoid any ambiguity between the title and the substance of that section."
8. The chronology of the change to the legislation was as follows:
- a) On 13 May 2014, Privacy International issued these proceedings, squarely raising the issue of the interaction between section 3 and section 10 CMA 1990 at paragraph 37 [A/17].
- b) On 5 June 2014, the Serious Crime Bill had its First Reading in the House of Lords. It contained, at clause 40, the amendments which were ultimately implemented as set out above.
- c) On 6 February 2015, the Respondents served an Open Response summarising the effect of sections 1 and 3 separately but not pleading to the issue identified in the Statement of Grounds. [A/68-69].
- d) On 3 March 2015, the SCA 2015 received Royal Assent.
- e) On 3 May 2015, the amendments made to the CMA 1990 by the SCA 2015 came into force.

Intelligence Services Act 1994

9. Section 3(1)(a) ISA provides that GCHQ's functions include "to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material". Section 3(2) ISA stipulates that

these functions are exercisable only in the interests of national security, the economic well-being of the United Kingdom, or the prevention or detection of serious crime.

10. Section 4(2)(a) ISA provides that one of the duties of the Director of GCHQ is to secure that *"no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings"*.

11. Section 5 ISA provides:

"(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.

(2) The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State –

(a) thinks it necessary for the action to be taken for the purpose of assisting, as the case may be, –

...

(iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and

(b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;

(c) is satisfied that satisfactory arrangements are in force under ...section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements."

12. Section 5(3) ISA provides that a warrant authorising interference with property within the British Islands can only be issued to GCHQ for its functions in respect of national security or the economic well-being of the UK. Within the UK, the Security Service handles the prevention and detection of serious crime, although GCHQ may in practice act on its behalf in actually carrying out interference.

13. In relation to section 5 warrants, section 6 ISA provides:

- a) at section 6(1), that warrants may only be issued under the hand of the Secretary of State or, in urgent cases, certain other officials;
- b) at section 6(2), that warrants issued by the Secretary of State expire after six months unless renewed;

- c) at section 6(3), that the Secretary of State may renew a warrant for 6 months at any time;
- d) at section 6(3), that the Secretary of State shall cancel a warrant *"if he is satisfied that the action authorised by it is no longer necessary"* (Section 6(4)).

14. In contrast, section 7 ISA provides:

"(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.

(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom.

(3) The Secretary of State shall not give an authorisation under this section unless he is satisfied –

(a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a function of the Intelligence Service or GCHQ; and

(b) that there are satisfactory arrangements in force to secure –

(i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of the Intelligence Service or GCHQ; and

(ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and

(c) that there are satisfactory arrangements in force under section 2(2)(a) or 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

(4) Without prejudice to the generality of the power of the Secretary of State to give an authorisation under this section, such an authorisation –

(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;

(b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified.

...

(9) For the purposes of this section the reference in subsection (1) to an act done outside the British Islands includes a reference to any act which—

(a) is done in the British Islands; but

(b) is or is intended to be done in relation to apparatus that is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus."

Section 7 also sets out provisions for the issue, renewal and cancellation of warrants, which broadly mirror those for warrants issued under section 5.

15. The power under section 7 to authorise acts outside the British Islands is much broader than the power in section 5. In particular:
- a) Section 7 is not limited to actions in respect of property or wireless telegraphy. It could be (and is) used to authorise a variety of other activities, including the recruitment of agents and the payment of bribes or inducements.
 - b) Section 7(4) permits the authorisation of acts by reference to a description of people or a class of operations, rather than merely in relation to "specified" property.

Police Act 1997

16. The ISA powers are very similar to the property interference powers available to the police under Part III of the Police Act 1997. The power to authorise interference is exercisable by senior police officers in their area, or more widely in certain cases:
- a) section 93(1)(a) provides: "*Where subsection (2) applies, an authorising officer may authorise ... the taking of such action, in respect of such property in the relevant area, as he may specify ...*";
 - b) section 93(2) establishes two cumulative criteria: first, that the authorising officer believes "*that it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime*", and second, that the authorising officer believes "*that the taking of the action is proportionate to what the action seeks to achieve*"; and
 - c) the Act also provides for authorisations to be reviewed by independent judicial Commissioners appointed under section 91, and makes specific provision in relation to the protection of legally privileged information: sections 97 and 98.

Property Interference Code of Practice

17. The Home Office has published a "Covert Surveillance and Property Interference Code of Practice" pursuant to section 71 RIPA [CM15/734, A1/10]. It has been referred to by the Respondents as the "Property Code", and that definition is adopted for convenience, although in fact it is concerned overwhelmingly with covert surveillance.
18. The version currently in force was published in December 2014, but, as the Respondents note *"in terms of property interference there is no material difference between the 2010 and the 2014 versions of the Code"*: [BA/95/§101].
19. Importantly:
 - a) The Property Code is only relevant to warrants issued under section 5 ISA 1994 [CM1/15/738/1.3]
 - b) The Property Code does not apply to warrants issued under section 7 ISA 1994.
 - c) The Secretary of State does not, even today, have statutory power to issue a Code in relation to section 7 ISA 1994.
20. The key provisions of the Property Code relating to property interference under section 5 ISA 1994 are:
 - a) Paragraph 7.18, which sets out information which should be provided in support of an application (including *"sufficient information to identify the property which the entry or interference with will affect [sic]"*);
 - b) Paragraph 7.19, which provides that in urgent cases the information may be submitted orally;
 - c) Paragraphs 7.36 to 7.42, which concern warrants for property interference by the intelligence services, and essentially state that the same information should be provided; and,
 - d) Section 8, which states that specified information pertaining to all authorisations *"shall be centrally retrievable within each public authority for a period of at least three years from the ending of each authorisation"*.

Draft Equipment Interference Code of Practice

21. The Home Office also published a draft Equipment Interference Code of Practice ("First Draft EI Code") on 6 February 2015. On the same day, the Respondents served their Open Response in these proceedings. The Respondents do not suggest this timing is a coincidence.
22. On 4 November 2015, the Respondents published a revised draft Equipment Interference Code ("Second Draft EI Code"). The Claimants have prepared a tracked changes version, which illustrates the significant changes between drafts.

23. The Second Draft EI Code remains a draft, and has not been brought into force. The most significant paragraphs of the Draft EI Code are as follows [CM1/14/708]:
- a) Paragraph 1.2: The EI Code takes precedence over the Property Code.
 - b) Paragraph 1.4: Although there is no power to make a Code about Section 7, as a matter of policy, the First Draft EI Code requires that it "must" be applied to equipment interference under section 7 (the wording in the Second Draft EI Code has reduced the mandatory "must" to a discretionary "should").
 - c) Paragraph 1.9 states: "*Equipment interference is conducted in accordance with the statutory functions of each Intelligence Service*", avowing the practice of CNE.
 - d) Footnote 1 defines "Equipment" very broadly. It "*may include, but is not limited to, computers, servers, routers, laptops, mobile phones and other devices*".
 - e) Section 3 contains purported safeguards for legally privileged and confidential information.
 - f) Section 4 sets out the procedures for authorising equipment interference under section 5 ISA 1994.
 - i) Paragraph 4.6 sets out the information which an application for a s.5 warrant must contain, including "*the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference*" and "*sufficient information to identify the equipment which will be affected by the interference*".
 - ii) Further, the First Draft EI Code requires application to describe "*any action which may be necessary to install, modify or remove software on the equipment*". The Second Draft EI Code added the words "*including an assessment of the consequences (if any) of those actions*".
 - g) Paragraph 6.3 provides that information obtained through equipment interference may be used as evidence in criminal proceedings.
 - h) Section 7 sets out the procedures for authorising equipment interference under section 7 ISA 1994.
 - i) Paragraph 7.6 states: "*An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations.*"
 - ii) Paragraph 7.11 reiterates "*An authorisation under section 7 may relate to a broad class of operations*", and paragraphs 7.12 to 7.14 make provision requiring "*internal approval to conduct operations under that authorisation in respect of equipment interference*".
 - iii) Paragraph 7.12 provides for internal approval of operations authorised under section 7 ISA by a "*designated senior official*".

Arrangements

24. Some limited parts of the internal 'arrangements' of GCHQ have been disclosed. In summary:
- a) The "Compliance Guide - Authorisations" states: *"The ISA warrant and authorisations scheme is a mechanism for removing liability that would otherwise attach to interference with property such as computers, phones and routers. This interference would otherwise be a criminal offence under the Computer Misuse Act."* In other words, the Respondents accept that in the absence of a valid authorisation, CNE violates domestic law [DD/1].
 - b) That Compliance Guide also states in relation to section 7 ISA: *"An ISA s.7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations. Wherever possible, GCHQ seeks to rely on class authorisations, including a class authorisation which permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant."*
 - c) In contrast, the section in relation to section 5 ISA makes no reference to the possibility of a warrant covering *"a broad class of operations"*; and,
 - d) An extract from the current Advanced Training for Active Operations states: *"CNE operations must be authorised under ISA s.5 or s.7, depending whether the target computer or network is located within or outside the British Islands."* The Guidance also notes the 5-day grace period under section 7, if the target computer is brought into the British Islands.

Annex 2 - Submissions of the Law Society in DRIPA litigation

IN THE COURT OF APPEAL
ON APPEAL FROM THE DIVISIONAL COURT
Bean LJ and Collins J

APPEAL NO C1/2015/2613

BETWEEN:

R (OAO (1) DAVID DAVIS MP, (2) TOM WATSON MP)

Claimants

-and-

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

SUBMISSIONS ON BEHALF OF
THE LAW SOCIETY OF ENGLAND AND WALES

1. One of the factors that led the Court of Justice of the European Union in *Digital Rights Ireland* (Case C-293/12) to hold that Directive 2006/24 was contrary to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("the Charter") was the absence of any exceptions in the Data Retention Directive for data relating to persons, "*whose communications are subject, according to rules of national law, to the obligation of professional secrecy.*" (§58 emphasis supplied)
2. Likewise, neither the Data Retention and Investigatory Powers Act 2014 ("DRIPA") nor the Regulation of Investigatory Powers Act 2000, which governs access to communications data retained under DRIPA ("RIPA"), include any exemptions in respect of persons subject to professional obligations of secrecy.
3. In her Detailed Grounds for Contesting the Claim at §85, the Home Secretary makes three claims:

- (1) First, that DRIPA, "does not extend to the content of any communications and consequently do not involved any interference with obligations of professional secrecy or confidence..."
 - (2) Second, that "the ability to use any data that did interfere with those interests in subsequent legal proceedings would be limited..."
 - (3) Third, that the Government has amended the draft RIPA Acquisition and Disclosure Code of Practice 2007, "to impose additional considerations as part of the process where it is known that communications data discloses contact between persons of certain professions and those they are advising".
4. The Acquisition and Disclosure Code of Practice 2007 (revised) - which is not legally binding and does not have the force of statute - now provides in paragraphs 3.72 - 3.74 that, "special consideration to necessity and proportionality" must be given when seeking communications data relating to a person who is a member of a profession that handles privileged or otherwise confidential information. Furthermore, "particular care" must be taken by designated persons when considering such applications.
 5. It is also said that it "may be possible to infer" an "issue of sensitivity" from the fact that a person has regular contact with a lawyer, journalist, doctor, minister of religion or Member of Parliament.
 6. This guidance is prefaced with the statement that:

"Communications data are not subject to any form of professional privilege - the fact that a communication took place does not disclose what was discussed, considered or advised."

7. Therefore not only are there no restrictions on the ability of persons to acquire communications data that is protected by professional confidence or legal professional privilege, but any person applying the revised Acquisition and Disclosure Code of Practice would conclude (1) that disclosure of communications data cannot infringe legal professional privilege; (2) that communications with lawyers have equivalent status in domestic law as communications with journalists, doctors, Ministers of religion (etc), and (3) that the sensitivity of communications with lawyers is a matter which merely requires particular care to be taken and "special consideration" (a vague notion) given to issues of necessity and proportionality.
8. The Law Society for England and Wales is concerned that these statements do not accurately reflect the obligations of professional secrecy recognised and upheld by the common law between a lawyer and their client.
9. Taking the Secretary of State's second point first, the fact that there are restrictions on the ability to use legally privileged material in legal proceedings fails to address the fact that legal professional privilege is a substantive right and not a mere rule of evidence. It provides an assurance of complete confidentiality in obtaining legal advice, and dealing with legal advisers in the context of litigation, and not merely an assurance that the communications will not be deployed in legal proceedings.

10. Thus:

- (1) In R v Derby Magistrates Court, Ex p. B [1996] AC 487 at 507 Lord Taylor of Gosforth stated:

"...a man must be able to consult his lawyer in confidence, since otherwise he might hold back half the truth. The

client must be sure that what he tells his lawyer in confidence will never be revealed without his consent. Legal professional privilege is thus much more than an ordinary rule of evidence, limited in its application to the facts of a particular case. It is a fundamental condition on which the administration of justice as a whole rests."

- (2) In *R (Morgan Grenfell & CO Ltd) v Special Commr of Income Tax* [2002] UKHL 21, [2003] 1 AC 563, 606-607 §7 Lord Hoffmann stated:

"LLP is a fundamental human right long established in the common law. It is a necessary corollary of the right of any person to obtain skilled advice about the law. Such advice cannot effectively be obtained unless the client is able to put all the facts before the adviser without fear that they may afterwards be disclosed and used to his prejudice."

11. As to the first and third points advanced by the Secretary of State, whilst it is generally the case that legal professional privilege attaches only to the content of communications and will not cover records of attendance or the identity of client⁵ this is by no means always so. Legal professional privilege will apply to information that may identify a client or their location, or the timing and frequency of contact with the lawyer, where such information is confidential.

12. Thus, information such as the dates of letters between solicitors and their clients have been held to be privileged because of the risk that their contents may be inferred: *Gardner v Irvin* (1878) 4 Ex D 49 at 83 (Cotton LJ).:

"I think that the plaintiffs are not entitled to have the dates of the letters and such other particulars of the

⁵ *R v Manchester Crown Court ex p. Roberts* [1999] 1 WLR 832 at 839 C-F: "A record of appointment made does involve a communication between the client and the solicitors' office but is not in my judgment, without more, to be regarded as made in connection with legal advice." (Bingham CJ).

correspondence as may enable them to discover indirectly the contents of the letters, and thus to cause the defendants to furnish evidence against themselves in this action." (approved Derby v Weldon (No 7) [1990] 1 WLR 1156)

13. This principle has been recognised as having wider application in several recent cases where the identity of a client and other information about them, such as their whereabouts or information which might indicate their movements, has been held to be protected by privilege. The underlying rationale is that if such information is not protected absolutely, some individuals would be deterred from contacting lawyers and obtaining legal assistance.
14. In JSC BTA Bank v Solodchenko & Ors (No 3) [2011] EWHC 2163, [2013] Ch 1 Mr Justice Henderson held that where a solicitor's client had provided his contact details under conditions of confidentiality, the justification for recognising legal professional privilege, namely, that a person should not be inhibited in seeking the aid of a lawyer, was just as squarely engaged as in relation to the advice itself. He said at §19:

"I can think of few things more likely to inhibit the exercise by a client of his fundamental right to seek legal advice than an order requiring his solicitor to disclose to an adverse party contact details which were supplied to the solicitor in strict confidence and for the sole purpose of enabling the client to communicate with the solicitor. In my view any such order would tend to undermine the relationship of confidence which must subsist between solicitor and client if the client is to be able to unburden himself freely to the solicitor."

15. In JSC Bank v Addleshaw Goddard LLP [2012] EWHC 1252 (Comm) the Claimants sought details of a conference call facility and of a special email account maintained by a firm of solicitors in order to communicate securely with their client, who was evading justice. It was submitted that the lines of communication between the solicitors and their clients were not themselves privileged or confidential (§16). The Court accepted that without more records of

appointments and contact details do not attract legal professional privilege. But on the facts of that case it held:

"The number and address have been provided by Addleshaw Goddard to the First Defendant in confidence. In my judgment the connections between the telephone number and the email address and the seeking and receiving of legal advice in the present case is clear and manifest." (§24)

16. Teare J held that despite the fact that the Defendant had gone into hiding in order to frustrate orders of the court, the right to have access to legal advice trumped this consideration. The Defendant was not an outlaw (§38).

17. Finally, in SRJ Person(S) Unknown being the author and commentators of Internet Blogs, D & Co [2014] EWHC 2293 (QB) Sir David Eady sitting as a High Court Judge dismissed an application for an order requiring solicitors to disclose the identity of their client. The information was sought by a company which had been the subject of leaks of confidential information on internet blogs by the anonymous employee, who was in breach of a court order. Sir David Eadie concluded:

"the information as to the Defendant's identity was indeed the subject of legal professional privilege and thus protected - Even if it were not there are powerful reasons not to override the duty of confidence. It was not simply a piece of neutral background information, as would generally be the case with a client's name, since both he and his solicitor were well aware that the Claimant was keen to establish his identity -". (§27)

18. The ability to obtain communications data relating to or revealing the contact that a lawyer has had with his or her client squarely engages the authorities referred to above. Those authorities make clear that such information can be protected by legal professional privilege and revealing such information would in some cases represent a violation of the fundamental right of every person to obtain legal representation without fear or inhibition.

19. It is of great importance that individuals are able to speak to their legal advisers without fear that such communications will be obtainable and capable of being used against their interests. That would have a chilling effect on the obtaining of legal advice and assistance.

20. The right to confidentiality between lawyer and client is deeply ingrained in the common law and it is absolute. It is, "the highest privilege recognised by the courts." (C. Passmore 1-005, *Privilege* 3rd ed. 2013, p.5). It is more fundamental even than the right of journalists to protection of their sources or of a Member of Parliament to speak openly with a constituent.

Conclusion

21. In *Digital Rights Ireland*, the CJEU indicated that any compulsory data retention regime must be accompanied by adequate restrictions on access to information which is protected by professional confidence under national law.

22. The law of England and Wales recognises that communications data relating to dealings between lawyers and their clients will in many cases be subject to legal professional privilege and affords that right the highest status.

23. Despite this, there are no restrictions on access to such data under applicable legislation. The non-statutory guidance provided in the revised Acquisition and Disclosure Code of Practice wrongly asserts that legal professional privilege cannot apply to communications data, fails to make clear the particular status of legal professional privilege and sets out no clear or appreciable limits on access to such material. It clearly falls short of the requirements contemplated by the CJEU.

TOM HICKMAN
Blackstone Chambers

7 October 2015

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK ("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB

Claimants

and

(1) THE SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH
AFFAIRS

(2) THE GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

THE RESPONDENTS' SKELETON ARGUMENT FOR OPEN
PRELIMINARY ISSUES HEARING 1-4 DECEMBER 2015

Privacy International and the Greenet Claimants are referred to below as "the Claimants".

The term "Respondents" is used below to refer to both Respondents in both Claims.

The IPT judgment in the Liberty/Privacy proceedings, [2014] UKIPTrib 13_77-H dated 5 December 2014, is referred to in this Response as "the Liberty/Privacy judgment".

Where appropriate references to the hearing bundles and authorities' bundles have been included in square brackets and with the authorities shown as [A1/A2].

INTRODUCTION

1. This skeleton addresses the Open preliminary issues of law (1-5) which have been agreed between the parties. For ease of reference when considering these submissions, the Respondents have set out in an Appendix to this skeleton argument the matters which go to make up the relevant legal regime including the relevant statutory provisions, Codes and oversight mechanisms. The abbreviations used in that Appendix have been adopted in this skeleton argument.
2. Over the last year the threat to the UK from international terrorism has continued to increase. The threat level currently stands at SEVERE which means an attack in the UK is highly likely. Six alleged terror plots targeting the UK have been stopped in the year prior to September 2015.¹
3. As is more than apparent from recent and tragic events in Paris, the principal terrorist threat derives from militant Islamist extremists, particularly in Syria and Iraq. Even before the attacks in Paris, it was clear that ISIL had emerged as the most violent of the terrorist groups operating in that region and that it was supported by foreign fighters from European countries². And central to ISIL's operational successes is "*an unprecedented quantity of extremist and terrorist propaganda*"³.
4. The task of defending the UK's interests and protecting its citizens in a digital age is becoming increasingly complicated and challenging; and it is in that regard that GCHQ plays a leading role given its expertise in digital communications technology. A combination of factors including the increasing use of the internet and social media by groups like ISIL, the unprecedented security of terrorist communications and the advent of ubiquitous encryption, mean that the work required to tackle national security threats is getting harder.
5. Thus GCHQ and the other intelligence agencies must develop innovative and agile technical capabilities to meet these serious national security challenges. Computer Network Exploitation (CNE) is one such capability⁴. Its importance

¹ See §7 of the first witness statement of Ciaran Martin, Director of Cyber Security at GCHQ dated 16 November 2015 – Open Bundle, Section B, p124.

² Ibid §§7-8

³ Ibid §§8 and 10

⁴ Ibid §20

relative to GCHQ's overall capabilities has been increasing in recent years and is likely to increase further⁵. Indeed, CNE may, in some cases, be the *only* way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country⁶; and without it GCHQ's ability to protect the UK from terrorism, cyber attack, serious crime (including child sexual exploitation) and a range of other threats would be seriously degraded.⁷

6. Contrary to the Claimants' assertions, CNE is lawful as a matter of domestic law and under the ECHR. There is a clear legal framework governing CNE activities, including the availability of warrants/authorisations under s.5 and s.7 ISA, supplemented in important respects by the CMA 1990, the HRA, the DPA, the OSA, the relevant Codes, GCHQ's internal arrangements and important oversight mechanisms. That regime is both accessible and has a proper basis in domestic law. It is a regime which provides for stringent safeguards if GCHQ wishes to carry out CNE activities. It is also proportionate given the need for CNE to be carried out to protect the public from serious terrorist and other threats.
7. The Claimants make extreme assertions about the intelligence gathering activities of GCHQ, including their alleged indiscriminate and arbitrary nature. Such assertions are flatly contradicted by eg. the recent report of the ISC⁸ and the conclusions of the Intelligence Services Commissioner (Sir Mark Waller) who described GCHQ staff as acting "*with the highest level of integrity and legal compliance*" in his 2013 report⁹ and noted in his 2014 report (with specific reference to the s.7 ISA process) that "*a great deal of thought was going into assessing the necessity of the activity in the national interest and to ensure privacy was invaded to the least degree possible*"¹⁰.
8. Thus, whilst the NCND principle precludes GCHQ from responding to the factual allegations which are made in these proceedings (and which have been addressed thoroughly in CLOSED), it is denied that GCHQ is engaged in any unlawful and indiscriminate mass surveillance activities.
9. As to the specific preliminary legal issues to be addressed in this OPEN hearing, the Respondents' position on each is in summary as follows:

⁵ Ibid §20

⁶ Ibid §31

⁷ Ibid §34

⁸ In their report "*Privacy and Security: A modern and transparent legal framework*" dated 12 March 2015 the ISC stated, *inter alia*, that "*We are satisfied that the UK's intelligence and security Agencies do not seek to circumvent the law – including the requirements of the Human Rights Act 1998, which governs everything that the Agencies do*" (see (v) Vol I/CMI/p562).

⁹ Ibid §72

¹⁰ Ibid §72

- Issue 1** GCHQ's CNE activities have been lawful as a matter of domestic law both before and after 3 May 2015. Prior to 3 May 2015 an act constituting an offence under s.3 CMA 1990 was capable of being authorised by a warrant or authorisation under the ISA (or a RIPA warrant). In addition, even if the effect of the Criminal Justice Act 1948 is of more than academic interest in these proceedings, that Act does not extend the territorial reach of the CMA 1990 for Crown servants.
- Issue 2** Section 5 ISA does permit the issue of a warrant where "property" is "specified" by description and such description may encompass more than one particular location, or item of property.
- Issue 3** The power under s.5 ISA to authorise interference with "property" does extend to intangible legal rights such as copyright.
- Issues 4/5** The regime which governs CNE is "*in accordance with the law/prescribed by law*" under Article 8(2)/Article 10(2) ECHR. It is sufficiently foreseeable, contains sufficient safeguards to protect against arbitrary conduct, is proportionate and this has been the case since 1 August 2009.

ISSUES 1-3 – DOMESTIC LAW

Issue 1: Prior to the amendments to the Computer Misuse Act 1990 ("CMA 1990") with effect from 3 May 2015, and after those amendments:

- a. was an act constituting an offence under s.3 CMA 1990 capable of being rendered lawful by a warrant issued under the Regulation of Investigatory Powers Act 2000 ("RIPA 2000") or a warrant or authorisation under the Intelligence Services Act 1994 ("ISA 1994")?*
- b. would the CNE activities of a Crown servant in the course of his employment, if committed in a foreign country or against assets or individuals located in a foreign country, have amounted to an offence under s.3 CMA 1990 as though the activities had been committed in England and against assets or individuals located in England?*

Is an offence under s.3 CMA 1990 capable of being rendered lawful by ISA/RIPA?

10. The Claimants contend that, prior to the amendments to the CMA 1990 on 3 May 2015, an act constituting an offence under s.3 CMA 1990 was not capable of being rendered lawful by any other enactment conferring powers of inspection/examination, search or seizure. In particular they assert that only lesser interferences, amounting to a breach of s.1 of the CMA 1990, could be

authorised by warrant under RIPA or the ISA (see §§37 and 41B(a) of Privacy's Re-Amended Grounds dated 13 July 2015¹¹). It appears to be accepted from Privacy's Grounds (adopted by the Greennet Claimants¹²) that since amendments to the CMA 1990 were made in May 2015, conduct under s.3 of the CMA 1990 could be authorised by a warrant under RIPA/the ISA (see §41B of Privacy's Grounds). Consequently any live issue is confined to the position pre-May 2015.

11. When enacting the ISA in 1994, after the coming into force of the CMA in 1990, Parliament made specific provision for the Intelligence Services, including GCHQ, to conduct activities which might otherwise be unlawful (whether under criminal or civil law), where the activity was authorised by s. 5 warrants or s. 7 authorisations. That is made expressly clear by the language of the ISA, in particular at s.5(1) and s.7(1)-(2):

"5(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.

"7(1) If, apart from this section; a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.

7(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom."(emphasis added)

12. As regards GCHQ's activities, Parliament was also clear when enacting the ISA that such activities should include the monitoring or *interference* with any equipment producing electromagnetic, acoustic and other emissions, as expressly stated to be part of GCHQ's statutory functions in s. 3(1)(a) of the ISA. That language plainly includes interferences which would otherwise constitute an offence, including impairing the operation of a computer under s.3 of the CMA 1990.
13. Consequently, the specific statutory scheme in the ISA is structured such that both s.5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that they are not civilly or criminally liable for such interferences, including under the CMA 1990.
14. S.10 of the CMA (prior to being amended on 3 May 2015) did not have the effect that only lesser interferences, amounting to a breach of s.1 of the CMA,

¹¹ See Open Bundle Part A, at p17 and p21.

¹² See Open Bundle Part A, p58 at §63.

could be authorised, including under the ISA or RIPA. That section was directed at “*certain law enforcement powers*” (see the title to s. 10) i.e. powers of inspection, search or seizure (eg. by the police)¹³. It did not purport to set out exhaustively the circumstances in which, what would otherwise be offences under the CMA, might be authorised eg. by the Intelligence Services when exercising their statutory functions including in the interests of national security and the prevention and detection of serious crime.

15. It follows that the amendments to s.10 CMA were clarificatory only. That is confirmed by the explanatory notes to that section and by the Home Office Fact Sheet to the Serious Crime Act 2015 (Part 2: Computer Misuse) and the Home Office Circular, both dated March 2015, which stated as follows:

“Section 10 of the 1990 Act contains a saving provision. It provides that the offence at section 1(1) of the 1990 Act has effect without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure; and in Scotland of any enactment or rule of law relating to powers of examination, search or seizure. The amendment to section 10 of the 1990 Act made by this section is a clarifying amendment. It is designed to remove any ambiguity over the interaction between the lawful exercise of powers (wherever exercised) conferred under or by virtue of any enactment (and in Scotland, rule of law) and the offence provisions. “Enactment” is expressly defined to provide certainty as to what this term includes. The title of section 10 of the 1990 Act has also been changed to remove the reference to “certain law enforcement powers” (see paragraph 12 of Schedule 4). This is to avoid any ambiguity between the title and the substance of that section.” (Explanatory Notes, emphasis added¹⁴)

“Section 44 clarifies the savings provision at section 10 of the 1990 Act and is intended to remove any ambiguity for the lawful use of powers to investigate crime (for example under Part 3 of the Police Act 1997) and the interaction of those powers with the offences in the 1990 Act. The changes do not extend law enforcement agencies’ powers but merely clarify the use of existing powers (derived from other enactments, wherever exercised) in the context of the offences in the 1990 Act.” (Home Office Fact Sheet)

“Section 44 clarifies section 10 of the CMA. Section 10 of the CMA contained a saving provision whereby criminal investigations by law enforcement agencies did not fall foul of the offences in the Act. However, section 10 pre-dates a number of the powers, warrant and oversight arrangements on which law enforcement now rely to conduct investigations, such as those in Part 3 of the Police Act 1997. The changes do not extend law enforcement agencies’ powers but merely clarify the use of the existing powers (derived from other enactments, wherever exercised) in the context of the offences in the CMA.” (Home Office Circular)

16. The interpretation contended for by the Claimants would lead to the absurd result that the authorisation mechanisms in the ISA could have no legal effect

¹³ See [A1/Tab 2]

¹⁴ See [A1/Tab 12]

unless there was an express savings provision in each relevant piece of legislation (whether governing criminal or civil liability), making clear that it was without prejudice to powers set out in any other enactment. That is manifestly inconsistent with the scheme of the ISA. It also elevates the status of savings provisions eg. in the CMA 1990, beyond that which is tenable. As has been recognised in the case law, savings provisions are a frequently unreliable guide to the provisions to which they attach, since savings provisions “are often included by way of reassurance, for the avoidance of doubt or for an abundance of caution” - see Lord Simon of Glaisdale in *Ealing London Borough Council v Race Relations Board* [1972] AC 342 at 363.

17. As to RIPA, it is to be noted that this would only be relevant if GCHQ's CNE activity also required a Part II RIPA warrant as well as an ISA warrant/authorisation eg. if intrusive surveillance was being carried out. But, in any event, RIPA came into force after the CMA 1990¹⁵ and Part II, makes clear that conduct to which that chapter applies is “lawful for all purposes” if it is authorised under that Chapter (see s. 21(2)¹⁶).
18. Accordingly, the submissions at §37 and §41B(a) of Privacy's Amended Grounds are wrong in law.

Does s. 48 of the Criminal Justice Act 1948 ('the CJA') extend the scope of territorial jurisdiction of the CMA 1990 for Crown servants?

19. The Claimants contend that s. 31 of the CJA¹⁷ has the effect of extending the territorial reach of the CMA 1990 for Crown servants. It is said that the effect of s.31 means that any breach of the CMA 1990 by a Crown servant abroad is deemed to have taken place in England and is within the territorial jurisdiction of the CMA 1990 (see §§37D, 37F, 41B(b) and 47A of Privacy's Amended Grounds).
20. The Respondents' primary submission is that the interface between the CJA and the CMA 1990 is entirely academic in circumstances where GCHQ has confirmed that, as a matter of practice, any CNE activities carried out abroad, or over a foreign computer, even if the relevant user is located in the United Kingdom, would be authorised by a s. 7 ISA authorisation (see §146C(a) of

¹⁵ Section 3 of the CMA 1990 came into force on 29 August 2000 and RIPA 2000 came into force on 2 October 2000.

¹⁶ See [A1/Tab 10]

¹⁷ Which provides as follows: “31(1) Any British subject employed under His Majesty's Government in the United Kingdom in the service of the Crown who commits, in a foreign country, when acting or purporting to act in the course of his employment, any offence which, if committed in England, would be punishable on indictment, shall be guilty of an offence and subject to the same punishment, as if the offence had been committed in England.” - see [A1/Tab 4]

the Respondents' Re-re-Amended Open Response¹⁸). The very purpose of s. 7 of the ISA is to provide for the granting of authorisations in respect of any act done outside the British Islands, where otherwise a person would be liable under the criminal or civil law of the UK. In addition, s. 7(9) of the ISA makes clear that such authorisations can relate to an act which is done in the British Islands, but which is or is intended to be done in relation to apparatus that is believed to be outside the British Islands.

21. In any event, it is not accepted that s. 31 of the CJA extends the scope of the territorial jurisdiction provisions in the CMA 1990 (see §37F of Privacy's Amended Grounds); nor are the broad assertions in §41B(b) of Privacy's Amended Grounds accepted as an accurate statement of the law¹⁹.
22. **First** the CMA 1990 contains specific and express provisions as to what territorial links with the jurisdiction are and are not necessary in order for an offence (eg. under s.3) to be committed. It is made clear in s.4(1) that, for the purposes of any offence under s.3 of the CMA 1990, it is immaterial (a) whether the act or event, proof of which is required for conviction, occurred in England and Wales or (b) whether the accused was in England and Wales at the time. But, as made clear by s.4(2), at least one significant link with the jurisdiction must exist in the circumstances of the case for the offence under s.3 to be committed. Prior to 3 May 2015 a significant link was present if (a) the accused was in England and Wales at the time when he did the unauthorised act or caused it to be done or (b) the unauthorised act was done in relation to a computer in England/Wales (see s.5(3))²⁰
23. In those circumstances the CMA 1990 is an example of a "purely domestic regulation" per Lord Parker CJ in *R v Naylor* [1962] 2 QB 527 i.e. it contains offences which are incapable of being committed where there are insufficient links with the jurisdiction and therefore are incapable of being transposed under the CJA 1948²¹.
24. The same would also apply, for example, to RIPA 2000 [A1/Tab 10]. Section 1(1) of that Act creates an offence of unlawful interception of a communication being transmitted by a public postal service or a public

¹⁸ At Open Bundle Part A p105

¹⁹ See Open Bundle Part A at p19 and p21

²⁰ and changes to s.5 brought about in May 2015 now mean that, for a s.3 offence, a significant link can also be established if the accused was outside the UK at the time the act constituting the offence occurred and (a) the accused was a UK national at the time or (b) the act constituted an offence under the law of the country in which it occurred (see s. 5(1A)) [A1/Tab 1].

²¹ See also *Cox v Army Council* [1963] AC 48 where Lord Parker CJ, in the context of s.70 of the Army Act 1955 (which contains similar provisions to s.31 CJA 1948) made clear at §71 that there would be certain acts or omissions punishable if done in England which cannot be reproduced by any equivalent occurrence taking place outside the country.

telecommunications system. Section 1(2) sets out the circumstances in which the interception of a communication being transmitted by a private telecommunications system is an offence and, in each case, the interception must take place in the United Kingdom. The definitions of 'private telecommunications system' and 'public telecommunications system' require a link to the United Kingdom. Thus it would be impossible to transpose an interception on a foreign telecommunications system carried out by a Crown servant acting abroad. Moreover to criminalise a Crown Servant working abroad would place that Crown servant in a worse position than a Crown servant working in the United Kingdom and would therefore not operate fairly and within reasonable limits.

25. **Secondly**, even if the CJA 1948 did apply, the question whether there was any liability under s. 31 of that Act, read with the CMA 1990, would depend upon the specific circumstances in question including, *inter alia*, the answers to the following key questions:

- (a) Whether the offence was contrary to the laws of the foreign country i.e. it would only be where the Crown Servant commits an offence contrary to the laws of the foreign country and which would be indictable in England, that section 31 of the CJA could apply. That follows from the fact that the section itself refers to the commission in a foreign country of an offence and avoids the absurdity of a Crown servant acting lawfully in the foreign country but exposing himself to criminal prosecution on return to England and Wales; and
- (b) Whether the offence was committed in a "foreign country" which bears a special meaning derived from the British Nationality Act 1948, which was repealed in part and replaced with the British Nationality Act 1981 and which means that section 31 of the CJA does not apply to (a) Commonwealth countries, (b) the Republic of Ireland and (c) British overseas territories.

26. Thus, this matter is academic; in any event, the Claimants' contention that the CJA 1948 extends the scope of territorial jurisdiction of the CMA 1990 for Crown servants is wrong in law; but, even if it were right, the matter could only be determined on a case by case basis and is incapable of being addressed in the general terms contended for by the Claimants.

Issue 2: Does s.5 ISA 1994 permit the issue of a 'class' or 'thematic' warrant, i.e. a warrant authorising certain acts or types of acts in general rather than by reference to specified property or wireless telegraphy?

27. In §41C of Privacy's Amended Grounds it is asserted that s.5 ISA warrants,

unlike s.7 ISA authorisations, are incapable of being issued on a "class" or "thematic" basis because of the requirement that the action and the property both be "specified".

28. The genesis for this complaint appears to be the 2014 report of the Intelligence Services Commissioner, Sir Mark Waller dated 25 June 2015. When dealing with ISA property interference warrants [Vol 1/CM1/p849ff], he stated as follows:

"• Thematic Property Warrants

I have expressed concerns about the use of what might be termed "thematic" property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers "to a particular act" or to "acts" undertaken in the course of an operation. However, section 5 is narrower referring to "property so specified".

During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or "thematic". I have expressed my view that:

- section 5 does not expressly allow for a class of authorisation; and*
- the words "property so specified" might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals.*

The agencies and the warrantry units argue that ISA refers to action and properties which "are specified" which they interpret to mean "described by specification". Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which "specifies" property by reference to a described set of persons, only being able to identify with precision an individual at a later moment.

I accept the agencies' interpretation is very arguable. I also see in practical terms the national security requirement.

The critical thing however is that the submission and the warrant must be set out in a way which allows the Secretary of State to make the decision on necessity and proportionality. Thus I have made it clear:

- a Secretary of State can only sign the warrant if they are able properly to assess whether it is necessary and proportionate to authorise the activity*
- the necessity and proportionality consideration must not be delegated*
- property warrants under the present legislation should be as narrow as possible; and*
- exceptional circumstances where time constraints would put national security at risk will be more likely to justify "thematic" warrants.*

This has led to one of the agencies withdrawing a thematic property warrant in order to better define the specified property. We remain in discussion to find a way to do so but I am anxious to ensure that they are not missing intelligence opportunities which might endanger national security.

I made five recommendations at each of the intelligence agencies and warranting units in relation to what might be termed thematic property warrants:

- 1. For any warrants which might be considered to be thematic to be highlighted in the list provided for my selection;*
- 2. The terms of a warrant and the submission must always be such as to enable the Secretary of State to assess the necessity and proportionality;*
- 3. The assessment of proportionality and necessity should not be delegated;*
- 4. Property warrants should be as narrow as possible but circumstances where time constraints and national security dictate may allow a more broadly drawn "thematic" warrant; and*
- 5. As the agencies and the Secretaries of State have made clear to me is the case, thematic or broadly drawn warrants should not be asked for simply for administrative convenience.*

I have recommended in general, and not just for thematic warrants, that the submission attached to the warrant should set out all the limitations applied to the use of the warrant and particularly should identify what action is being taken to minimise intrusion into privacy." (see pages 18-19)

29. It is to be noted that the terms "thematic" and "class" as used by Privacy do not form part of the statutory requirements for the issue of a warrant under s.5. Insofar as the term "thematic" used by Privacy refers to the usage by the Commissioner the report set out above, the Respondents position is as follows:
30. **First** s.5(1) ISA provides: "No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section." That provision does not delimit the scope of a warrant to any single piece of property or single instance or method of entry on to or interference with property or wireless telegraphy.
31. **Secondly** by s.5(2) the Secretary of State may, on an application by GCHQ, issue a s.5 warrant authorising "the taking, subject to subsection (3) ..., of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified". Therefore if and insofar as action and/or property and/or wireless telegraphy is specified in a s.5 warrant, the warrant will be valid as regards that specification.
32. **Thirdly** whether action and/or any property and/or wireless telegraphy is "specified" in a warrant will depend upon the words used in the particular warrant. The phrase "any property so specified" in s.5(2) is not to be read as precluding the Secretary of State from issuing a warrant save in relation to a particular operation against a particular piece of property. Given the terms of

s.5 of the ISA "property" can be "specified" in a s. 5 warrant by description and such description may encompass more than one particular location or item of property eg. with reference to a described set of persons.

33. The Secretary of State can only sign a warrant if satisfied that the activity thereby authorised is necessary and proportionate in accordance with the statutory tests and that there are satisfactory arrangements in force with regard to the disclosure of information obtained under the warrant (see s.5(3)). In making that assessment the Secretary of State is required to consider whether what is sought to be achieved by the warrant could be achieved by other means (s.5(2A)). As noted by the Commissioner there may be circumstances in which the requirements of national security mean that it is simply not possible to specify with precision a defined individual, as opposed to eg. a set of persons to which the warrant relates. But there is nothing in the language of the ISA which would preclude a warrant being issued on that basis provided the statutory tests are otherwise satisfied.
34. In those circumstances it is submitted that s.5 does permit a property to be specified in a warrant by description and it is not accepted that any warrants where this may have occurred were unlawful.

Issue 3: Does the power under s.5 ISA 1994 to authorise interference with "property" encompass physical property only, or does it also extend to intangible legal rights, such as copyright?

35. The only stated basis for the Claimants' contention that a warrant under section 5 ISA can pertain to interference with only physical property is that ss.5(3) and (3A) refer to interference with property "in the British Islands".²² That reference is of no assistance:
 - (a) **First**, the natural reading of the phrase is that it is employed to distinguish between property in and outside the UK for the purposes of the scope of s.5 and not types of property: it is a phrase intended to limit the geographical scope of interference, not the type of property with which interference could occur.
 - (b) **Secondly**, if Parliament had intended to delineate different types of property and limit the scope of the term, it could have done so but chose not to.²³

²² Privacy Re-Amended Statement of Grounds §41D.

²³ In contrast, for example, the Criminal Damage Act 1971 is specifically limited to "tangible" property by s.10.

- (c) **Thirdly**, the supposed tension between the use of the phrase “in the British Islands” and coverage of intangible property by section 5 is difficult to understand in circumstances where, in particular, copyright is a territorially delimited right in domestic law and, therefore, the reference is consistent with that limitation.²⁴
- (d) **Fourthly**, reading the term “property” as being qualified by the term “physical” would result in an anomalous position in practice on the Claimants’ own case. The sort of interference contemplated by the Claimants ie. modification or adaptation of a computer programme on a target computer, would itself be *lawful* under a warrant: the reconfiguration of electrons on a computer so as to modify the manner in which it operated would be a physical interference which is contemplated to be permissible. The warrant would permit such action. Yet simultaneously, the Claimants also say that the very same rearrangement of electrons is also unlawful because it affects an intangible property right. There is no reason to suppose that Parliament intended such a state of affairs to be capable of arising when the overall purpose of the section is to enable lawful interference.

36. Thus the contention that s.5 warrants could not cover interferences with intangible property are unfounded.

37. But further and in any event, the Claimants fail to recognise that even if a s.5 warrant did not cover a potential inference with copyright, no basis for alleging any breach of copyright has been put forward:

- (a) §41E of Privacy’s Amended Grounds²⁵ is wholly vague as to the nature or type of the alleged interference with copyright and it is inadequately pleaded (by reference to other allegations made or otherwise).
- (b) The Claimants purport to rely on EU Directive 2001/29 [A1/Tab 14] but its relevance is not understood. Notwithstanding that in their Amended Open Response of 25 September 2015 the Defendant explained that the relevant law of copyright is the domestic law of England and Wales and no breach thereof is alleged, no further explanation of the Claimants’ position has been proffered. As made clear in the Open Response, it has not been contended that the United Kingdom has failed to implement Directive 2001/29 in domestic law. It is noted that Directive 2001/29 was implemented in the United

²⁴ In particular Part I of the Copyright, Designs and Patents Act 1988 extends only to England and Wales, Scotland and Northern Ireland.

²⁵ See Open Bundle Part A/p22

Kingdom in particular in the Copyright Designs and Patents Act 1988 (as amended).

- (c) Further or alternatively, insofar as it is relevant it is denied that:
- i. the actions of the Defendant pursuant to the protection of national security interfere with any rights protected under Directive 2001/29; and/or
 - ii. any interference with such rights by the actions of the Defendants is unlawful or disproportionate.

38. The further references in §41F of Privacy's Amended Grounds do not assist the Claimants' case. The judgment Case C-293/12 *Digital Rights Ireland* [A2/Tab 26] was not concerned with copyright, did not consider standards required for derogations under Directive 2001/29 (albeit the relevance of which is not understood – see above) and did not purport to lay down “the standard required to justify a derogation from EU law rights” whether in relation to “surveillance” or otherwise. Indeed, it is noted that on 20 November 2015 the Court of Appeal gave a judgment in *Secretary of State for the Home Department v Davis & Watson* [2015] EWCA Civ 1185 in which it stated that its provisional view was that the judgment in *Digital Rights Ireland* did not lay down mandatory requirements even in relation to the matters with which it was directly concerned and ordered a preliminary reference to the CJEU in that regard.
39. Thus not only have the Claimants failed to make good their statutory interpretation contention, given the nature, scope and derogations available under copyright law they have failed to put forward any good basis for any breach of copyright.

ISSUES 4 AND 5 - ECHR

Is the regime which governs Computer Network Exploitation (“the regime”) “in accordance with the law” under Article 8(2) ECHR / “prescribed by law” under Article 10(2) ECHR? In particular:

- a. *Is the regime sufficiently foreseeable?*
- b. *Are there sufficient safeguards to protect against arbitrary conduct?*
- c. *Is the regime proportionate?*
- d. *Was this the case throughout the period commencing 1 August 2009?*

Article 8 ECHR – the principles

40. As the Tribunal held at §37 of its judgment in *Liberty/Privacy* [A2/Tab 22], in

order for an interference to be “in accordance with the law”:

“i) there must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action.

ii) the nature of the rules must be clear and the ambit of them must be in the public domain so far as possible, an “adequate indication” given (Malone v UK [1985] 7 EHRR 14 at paragraph 67), so that the existence of interference with privacy may in general terms be foreseeable...”

See also *Bykov v. Russia*, appl. no. 4378/02, 21 January 2009, at §78 [A2/Tab 31], quoted at §37 of *Liberty/Privacy*.

41. As the Tribunal also noted in *Liberty/Privacy*, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §§38-40 and §137). See also in that respect, *Malone v UK* (1984) 7 EHRR14 at §§67-68m [A2/Tab 42], *Leander v Sweden* [1987] 9 EHRR 433 at §51 [A2/Tab 40] and *Esbester v UK* [1994] 18 EHRR CD 72 [A2/Tab 33], quoted at §§38-39 of *Liberty/Privacy*. Thus, as held by the Tribunal in the *British Irish Rights Watch* case dated 9 December 2004 [A2/Tab 21] (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87): “foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security...” (§38)
42. Thus, the national security context is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the *Liberty/Privacy* judgment [A2/Tab 22]). That is not least because the ECtHR has consistently recognised that the foreseeability requirement “cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly”: *Malone v. UK*, §67 [A2/Tab 42]; *Leander v. Sweden*, §51 [A2/Tab 40]; and *Weber and Saravia v Germany* (2008) 46 EHRR SE5, §93 [A2/Tab 49].
43. As to the procedures and safeguards which are applied, two points are to be noted.
44. **First** it is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* [A2/Tab 42] and §78 of *Bykov* [A2/Tab 31]; and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy* [A2/Tab 22]. Hence the reliance on the Code in *Kennedy v United Kingdom* [2011] 52

EHRR 4 at §156 [A2/Tab 36] and its anticipated approval in *Liberty v United Kingdom* [2009] 48 EHRR at §68 [A2/Tab 41] (see §118 of *Liberty/Privacy* and also *Silver v United Kingdom* [1983] 5 EHRR 347).

45. **Secondly** it is permissible for the Tribunal to consider rules, requirements or arrangements which are “below the waterline” i.e. which are not publicly accessible. In *Liberty/Privacy* the Tribunal concluded that it is “not necessary that the precise details of all of the safeguards should be published, or contained in legislation, delegated or otherwise” (§122), in order to satisfy the “in accordance with the law” requirement; and that the Tribunal could permissibly consider the “below the waterline” rules, requirements or arrangements when assessing the ECHR compatibility of the regime (see §§50, 55, 118, 120 and 139 of *Liberty/Privacy*). At §129 of *Liberty/Privacy* the Tribunal stated:

“Particularly in the field of national security, undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise...This is particularly so where:

- i. *The Code...itself refers to a number of arrangements not contained in the Code...*
- ii. *There is a system of oversight, which the ECHR has approved, which ensures that such arrangements are kept under constant review.”*

46. Those conclusions were reached in the context of the s. 8(4) RIPA interception regime. They are equally applicable to the equipment regime where the relevant Codes both refer expressly to undisclosed statutory “arrangements” under the ISA (see eg. §1.3 of the EI Code [Vol 1/CM1/p707] and §7.38 and §9.7 of the Property Code²⁶ [Vol 1/CM1/p809/p815]) and where there is similar oversight by the Intelligence Services Commissioner.
47. In the context of interception, the ECtHR has developed a set of minimum safeguards in order to avoid abuses of power. These are referred to as ‘the *Weber* requirements’. At §95 of *Weber* [A2/Tab 49], the ECtHR stated:

“In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.” (numbered items added for convenience, see §33 of *Liberty/Privacy*)

²⁶ And see §2.19 of the 2002 version of the Property Code.

(And see also *Valenzuela Contreras v Spain* (1999) 28 EHRR at §59)

48. However it is important to recognise what underpins the *Weber* requirements, as highlighted at §119 of the *Liberty/Privacy* judgment. In particular, §106 of *Weber* states as follows:

“The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant’s right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security (see, inter alia, Klass and Others, cited above, p. 23, § 49; Leander, cited above, p. 25, § 59; and Malone, cited above, pp. 36-37, § 81). Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see Klass and Others, cited above, pp. 23-24, §§ 49-50; Leander, cited above, p. 25, § 60; Camenzind v. Switzerland, judgment of 16 December 1997, Reports 1997-VIII, pp. 2893-94, § 45; and Lambert, cited above, p. 2240, § 31). This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law (see Klass and Others, cited above, pp. 23-24, § 50).” (emphasis added)

49. This emphasis on the need to consider all the circumstances of the case was recently reiterated by the ECtHR in *RE v United Kingdom* (Application No. 62498/11) 27 October 2015 at §127 [A2/Tab 44]. In that case, because of the “*extremely high degree of intrusion*” involved in the surveillance of legal consultations it expected the same safeguards to be in place as in an interception case, at least insofar as those principles could be applied to the surveillance in question (see §131). On the specific facts of that case, a breach of Article 8(2) ECHR was found given that the surveillance regime as it applied to legal consultations did not contain sufficient provisions as regards the examination, use and storage of the material obtained and the precautions to be taken when communicating the material to other parties or erasing/destroying the material (see §§138-141). The ECtHR contrasted the provisions in Part I of RIPA and the Interception Code, which the Court approved in *Kennedy*, and concluded that they provided an example of the type of provisions which were required in this context.
50. The Tribunal in *Liberty/Privacy* placed considerable reliance on **oversight mechanisms** in reaching their conclusion that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8 compliant. In particular:

- (a) The role of the Commissioner and “his clearly independent and fully implemented powers of oversight and supervision” have been long recognised by the ECtHR, as is evident from *Kennedy* at §§57-74, 166, 168-169 [A2/Tab 36] (see *Liberty/Privacy* at §§91-92 [A2/Tab 22]). Whilst the Tribunal will, of course, form its own judgment about the effectiveness of his supervision in the CNE context, it is clear that this is potentially a very important general safeguard against abuse. In *Liberty/Privacy* the Tribunal relied, in particular, on his duty to keep under review the adequacy of the arrangements required by statute and by the Code, together with his duty to make a report to the Prime Minister if at any time it appeared to him that the arrangements were inadequate.
- (b) The advantages of the Tribunal as an oversight mechanism were emphasised at §§45-46 of *Liberty/Privacy*, including the “very distinct advantages” over both the Commissioner and the ISC for the reasons given at §46 of the judgment.
- (c) In addition the ISC was described as “robustly independent and now fortified by the provisions of the JSA” (see §121 of *Liberty/Privacy*) and therefore constituted another important plank in the oversight arrangements.
51. Consequently there is a need to look at all the circumstances of the case and the central question under Art. 8(2) is whether there are:

“...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.” (see §125 of the *Liberty/Privacy* judgment)

Application of those legal tests to the Equipment Interference Regime

Preliminary matters

52. Prior to considering the detailed safeguards which apply to the Equipment Interference regime, the Respondents make three preliminary points.
53. **First**, it is not accepted, even on the basis of the factual assertions made in the Claimants’ Grounds (which are neither confirmed nor denied), that such activities are factually or legally more intrusive than other forms of surveillance or data-gathering, including the interception of communications (see §§42-46 of the Privacy Grounds and §§55-57 of the Greennet Grounds).

54. As stated at §42-44 of Ciaran Martin's first witness statement [**Open Bundle, Part B/p124ff**], whilst it is accepted that CNE operations can be highly intrusive, they are not in general more intrusive than other operations conducted by GCHQ eg. under RIPA 2000 or the ISA. For example Part II of RIPA permits public authorities to engage in intrusive surveillance. A listening device directed at say a bedroom clearly has the potential to obtain information of an extremely private and personal data. In addition with the advent of certain types of remote storage, much of the material referred to in the Claimants' complaints could potentially be available via interception under Part I of RIPA.
55. The ECtHR has expressly referred to the fact that "*rather strict standards*" apply in the interception context, but do not necessarily apply in other intelligence-gathering contexts: *Uzun v. Germany* (2011) 53 EHRR 24, at §66 [**A2/Tab 48**] and see also *McE v. Prison Service of Northern Ireland* [2009] 1 AC 908, *per* Lord Carswell at §85 [**A2/Tab 24**]. In *RE v United Kingdom* the ECtHR held that an "*extremely high degree of intrusion*" involved in the surveillance of legal consultations meant that the same safeguards had to be in place as in the interception context.
56. Here there is no factual or legal justification for asserting that an even stricter set of standards ought to apply to equipment interference activities, over and above those which would apply eg. in an interception case.
57. Therefore in circumstances where GCHQ accepts that these activities represent a similar level of intrusiveness in Article 8 ECHR terms to eg. interception under Part I of RIPA, it is acknowledged that consideration of the *Weber* requirements is necessary as part of an assessment of all the circumstances of the case.
58. **Secondly**, as has already been made clear, GCHQ does not seek to carry out indiscriminate mass surveillance activities of the sort alleged by the Claimants both in the Grounds and in their witness evidence (see §36 of Ciaran Martin's first statement [**Open Bundle Part B/p131-132**] and see also §7 of his third statement dated 24 November 2015). Such activities are precluded by the clear statutory framework which regulates GCHQ's activities. CNE activities must be authorised by the Secretary of State and are subject to strict tests of necessity and proportionality and legitimate aim as set out in the ISA. These authorisations and the internal processes which are in place to manage these activities are subject to independent scrutiny by the Intelligence Services Commissioner and the ISC.
59. It follows from this that many of the examples given in the Claimants'

evidence about the possibilities created by CNE techniques bear no relation to the reality of GCHQ's activity and/or would be unlawful having regard to the relevant statutory regime.

60. It also follows that the Tribunal must exercise caution when approaching the assumed facts for the purposes of testing the legal issues. For very good reason GCHQ is unable to confirm or deny what particular CNE techniques/capabilities it has or what type of CNE operations are conducted by it. It has therefore been extremely difficult for GCHQ to engage in OPEN with the assumed facts without breaching NCND (although it has sought to do so in its CLOSED evidence).
- (a) For example §6(e) refers to *"the use of CNE in respect of numerous devices, servers or networks without first having identified any particular device or person as being of intelligence interest"*. If that were taken literally it might suggest that GCHQ would engage in CNE activities on a speculative/trawling basis, without any proper justification. But that would clearly be precluded by the legislation and the core requirements of necessity and proportionality. Consequently it is only having considered the CLOSED evidence about GCHQ's actual activities that the Tribunal can properly assess whether the activities are met with adequate safeguards and are proportionate.
- (b) Similarly §6(d) of the assumed facts refers to *"the use of CNE in such a way that it creates a potential security vulnerability in software or hardware, on a server or a network"*. Here GCHQ can respond (at least in general terms) and has made clear in Mr Martin's first statement that operations are carried out in such a way as to minimise that risk (see §41 [Open Bundle, Part B/p132-133]). To leave targets open to exploitation by others would increase the risk that privacy would be unnecessarily intruded upon and would also increase the risk of GCHQ's sensitive tools and techniques being identified. Consequently GCHQ does not intrude into privacy any more than is necessary to carry out its functions and takes steps to to minimise these risks. It also carries out important internet safety and cyber-security activities, including detecting and disclosing security vulnerabilities, as explained in §§40-41 of Mr Martin's first statement [Open Bundle, Part B/p132-133]. Consequently the reality of GCHQ's activities is inadequately reflected in a bald statement that CNE may be used in such a way that it creates potential security vulnerabilities in software or hardware or a server/network.
- (c) In addition §6(b) refers to the *"creation, modification or deletion of*

information on a device, server or network". In that regard whilst GCHQ recognises that CNE activity could theoretically change the material on a computer eg. by the installation of an implant which would itself amount to a change, it would be neither necessary nor proportionate, nor operationally sensible, to make more than the most minimal and to the greatest extent possible, transient, changes to targeted devices (see §46 of Mr Martin's first statement [**Open Bundle, Part B/p133**]). Consequently the extent to which a CNE operation involves the creation, modification or deletion of information would always have to be part of the necessity and proportionality justification.

61. **Thirdly**, contrary to the assertion made in the Claimants' Grounds, there is a clear legal framework governing any equipment interference activities, as set out in detail earlier in this Response. The availability of warrants under s. 5 and authorisations under s. 7 of the ISA, do provide a firm legal framework which is supplemented in important respects by the CMA, HRA, the DPA, the OSA, the relevant Codes and GCHQ's internal arrangements. That statutory scheme, in common with the interception regime in RIPA, makes certain activities an offence (as is the case eg. in s. 1 of RIPA which makes it an offence, without lawful authority to intercept certain communications) but is coupled with a regime for the issuing of warrants/authorisations which render the activity lawful if strict conditions are satisfied. The suggestion that the availability of a warrant under the ISA "*simply cancels any unlawfulness*" is a misrepresentation and an over-simplification of the statutory scheme and the safeguards which are inherent within it.
62. The Equipment Interference regime is therefore "accessible" and has a basis in domestic law, in that it consists of provisions in primary legislation and in relevant Codes and also in relevant internal arrangements/safeguards which are applied by GCHQ. The Claimants' argument that there is no relevant legal regime that regulates the circumstances in which and the conditions in which GCHQ may interfere with equipment is therefore untenable.

Compatibility of the regime since February 2015

Weber (1) and (2)

63. As noted by the Tribunal at §115 of *Liberty/Privacy* [A2/Tab 22], *Weber* (1) and (2) overlap and therefore can be taken together.
64. These requirements i.e. the "offences" which may give rise to a warrant/authorisation and the categories of people liable to be involved, are clearly satisfied by s. 5 and s.7 of the ISA, as read, in particular, with §1.6,

65. As noted in *RE v United Kingdom* [A2/Tab 44], although sufficient detail should be provided of the nature of the offences in question, the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to the activity (see §132). Consequently terms such as “national security” and “serious crime”²⁷ are sufficient (see *RE* at §133 and §116 of the *Liberty/Privacy* judgment [A2/Tab 22]). In addition it was also accepted in *RE* that it may not be necessary to know in advance precisely what individuals will be affected eg. by the surveillance measures in each case. Nevertheless given that the application was required to set out in full the information that was known and the proportionality of the measure was subsequently scrutinised in detail, no further clarification of the persons liable to be subject to the measures could reasonably be required (see §136).
66. As to the procedures for authorising CNE activities, these are addressed specifically at Chapter 4 of the EI Code [Vol 1/CM1/p719ff]. In particular, at §4.6 a detailed set of criteria are identified in terms of the information which is provided to the Secretary of State when applying for the issue or renewal of a s.5 warrant and this information must also be provided, where reasonably practicable, for any section 7 authorisation (see §7.7 and §7.2 of the EI Code [Vol 1/CM1/p726-727]). That paragraph states:

“4.6 An application for the issue or renewal of a section 5 warrant is made to the Secretary of State. Each application should contain the following information:

- *the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference;*
- *sufficient information to identify the equipment which will be affected by the interference;*
- *the nature and extent of the proposed interference, including any interference with information derived from or related to the equipment;*
- *what the operation is expected to deliver and why it could not be obtained by other less intrusive means;*
- *details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected.*
- *whether confidential or legally privileged material may be obtained. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege or confidential personal information, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;*
- *details of any offence suspected or committed where relevant;*
- *how the authorisation criteria (as set out at paragraph 4.7 below) are met;*
- *what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);*
- *where an application is urgent, the supporting justification;*

²⁷ as found in the ISA (see, for GCHQ, s5(3) and s.7(3) of the ISA read with s.3(2)).

- *any action which may be necessary to install, modify or remove software on the equipment;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results.”*

It is to be noted that a similar provision to §4.6 above (i.e. §5.2 of the Interception Code) was described in *Liberty/Privacy* as “impressive” at §116(iv) [A2/Tab 22].

67. In addition, §4.7 contains a checklist of matters about which the Secretary of State must be satisfied/consider before issuing a warrant/authorisation including:
- being satisfied that it is necessary for the purposes of carrying out the intelligence services functions;
 - being satisfied that it is proportionate;
 - taking into account whether there are other means by which the information could reasonably be obtained; and
 - being satisfied that there are satisfactory arrangements in place as regards disclosure of any information obtained.
68. These provisions are also accompanied by detailed guidance in Chapter 2 of the Code [Vol 1/CM1/p711] on the requirements of necessity and proportionality in this context, including issues such as collateral intrusion and the need to consider less intrusive alternatives. General best practice guidance is also given at §§2.16 and 2.17 including making sure that there is a designated senior official within each of the Intelligence Services responsible for, inter alia, the integrity of the process to authorise equipment interference and engagement with the Commissioner.
69. More specifically, in terms of the procedures for s.7 authorisations:
- As noted above, the same procedures and safeguards apply as under s.5 ISA (§7.2 EI Code [Vol 1/CM1/p726]), including the detailed authorisation procedures in Chapter 4. In particular any application for a s.7 authorisation to the Secretary of State should contain the same information, as far as reasonably practicable in the circumstances, as an application for a s.5 warrant (§7.6 EI Code [Vol 1/CM1/p726-727]).
 - Once a s.7 authorisation has been made by the Secretary of State, which may be specific to a particular operation or user or may relate to a broader class of operations (§7.6 EI Code Vol 1/CM1/p726-727)), the Code makes clear that it is necessary for internal approval to

conduct operations under that authorisation to be sought from a designated senior official.

- (c) In circumstances where the equipment interference is likely or intended to result in the acquisition of confidential information, authorisation should be sought from an Annex A approving officer, which in GCHQ's case is a Director of GCHQ (see §7.12 EI Code Vol 1/CM1/p727).
- (d) Clear guidance is provided as to what information should be included in any application for an internal approval at §7.13 of the EI Code [Vol 1/CM1/p728] which essentially replicates and requires the same information as any application to the Secretary of State for a s.5 warrant. It states:

"The application for approval must [should²⁸] set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer must [should²⁹] be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer must consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations."

As is evident from this final part of §7.13, there is specific provision for the FCO to be consulted, or the endorsement of the Secretary of State obtained for particularly sensitive operations.

- 70. It is therefore submitted that the regime is sufficiently clear both as to the nature of the offences which may give rise to equipment interference activity and the categories of person liable to be subject to such measures.
- 71. It is also to be noted, in terms of substantive safeguards, that there are additional layers of assurance built into the s.7 approvals process including:
 - (a) An increasing emphasis on providing detailed information to the Secretary of State about the type of CNE activities covered by s.7 class authorisations. For example since July 2014 GCHQ has copied to the

²⁸ "should" now appears in the November 2015 version of the Code

²⁹ Ibid

FCO all of its internal s.7 approvals for CNE operations which were given pursuant to the class authorisation and serious attention is given to this by senior Ministers and their advisors including, *inter alia*, meetings to discuss individual warrants/authorisations (see §63 of Ciaran Martin's first statement [Open Bundle/Part B/p138] and §§9-11 of his third statement).

- (b) Within GCHQ there is an internal specialist risk assessment panel, involving a range of relevant technical, operational and policy leads, which provides expert oversight and assurance that the tools and techniques being used and the way in which they are used, present an acceptable level of technical and operational risk. This includes providing an audit trail and a 'history' of decisions which for example are used to inform risk assessment statements in s.7 approval requests and political decisions (see §65 of Ciaran Martin's first witness statement).
- (c) In accordance with §7.13 of the EI Code discussed above [Vol 1/CM1/p728], if an operation is judged to present a significant risk, the proposal will be submitted to FCO officials or the Secretary of State and GCHQ will also seek FCO legal advice if a proposed operation involves issues of international law (see §66 of Ciaran Martin's first witness statement [Open Bundle/Part B/p138]).

Weber (3)-(6)

- 72. The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are dealt with in the combination of the ISA, the CTA, the DPA, the HRA, the OSA and in Chapters 2, 4, 6 and 7 of the EI Code and GCHQ's internal arrangements.
- 73. As to **duration**:
 - (a) The ISA makes sufficient provision for the duration of s.5/s.7 warrants/authorisations and the circumstances in which they can be renewed or should be cancelled – see s.6 and ss.7(5)-7(7) of the ISA (at [A1/Tab 7] and referred to at §§23-26 and §§33-35 of the Appendix to this skeleton).
 - (b) In addition the EI Code contains important provisions on reviewing warrants and the frequency of reviews, which apply equally to s.7 activity (see §§2.13-2.15 and §7.2 [Vol 1/CM1/p712/p726]) and for renewals and cancellations of s.5 warrants (see §§4.10-4.13 [Vol 1/CM1/p721]) and for renewals of s.7 authorisations (see §§7.15-7.16

[Vol 1/CM1/p728]). It is to be noted that in *RE v United Kingdom* similar provisions in Part II of RIPA and in the revised Property Code were considered to be "sufficiently clear" see §137 [A2/Tab 44].

- (c) In addition, in terms of the s.7 internal approvals process, the EI Code makes specific provision for regular reviews to ensure that operations continue to be necessary and proportionate. At §7.14 it states [Vol 1/CM1/p728]:

"All internal approvals must [should³⁰] be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case."

74. In addition there are detailed safeguards which apply which mirror the safeguards in s.15 of RIPA in the interception regime, as regards the **handling, dissemination, copying, storage, disclosure and security arrangements** for information obtained as a result of equipment interference.

- (a) These include detailed safeguards in Chapter 6 of the EI Code (see the Appendix to this skeleton at §62ff and Vol 1/CM1/p723-725) which include, *inter alia*, provisions which:

- i. limit the number of persons to whom any information is disclosed to the minimum necessary for the proper discharge of the Intelligence Services functions, including applying the 'need to know' principle (EI Code §§6.6-6.7);
- ii. limit the circumstances in which information obtained by equipment interference can be copied (EI Code §6.8);
- iii. require information obtained by equipment interference to be handled and stored securely and inaccessible to persons without the required level of security clearance (EI Code §6.9 and §6.11);

- (b) Further GCHQ must ensure that there are internal arrangements in force, which are approved by the Secretary of State, for securing that the requirements set out in Chapter 6 of the EI Code are satisfied in relation to all information obtained by equipment interference (see §6.4 of the EI Code) and these internal arrangements should be made available to the Commissioner (see §6.5 of the EI Code).

³⁰ Ibid

(c) Any information emanating from equipment interference can be used by GCHQ only in accordance with s.19(2) of the CTA as read with the statutory definition of GCHQ's functions (in s. 3 of the ISA) and only insofar as that is proportionate under s.6(1) of the HRA (see the Appendix to this skeleton at §§8-10 and §§101-104).

(d) Pursuant the DPA, GCHQ is not exempt from an obligation to comply with the seventh data protection principle, which provides:

*7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*³¹

Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question (see the Appendix to this skeleton at §§106-108).

(e) Any disclosure eg. deliberately in breach of the "arrangements" for which provision is made in s.4(2)(a) of the ISA would be a criminal offence under s.1(1) of the OSA which could attract imprisonment of up to two years (see the Appendix to this skeleton at §109) .

(f) Further a member of the intelligence service will commit an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the ISA read with s.1(1)). Conviction may lead to imprisonment of up to 3 months. Consequently this statutory obligation is relevant to the publicly available safeguards for the handling and security arrangements for information obtained through equipment interference (see the Appendix to this skeleton at §110).

(g) Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 at §§191-194).

³¹ The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

- (h) Finally any disclosure of such information must satisfy the constraints imposed in ss. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

75. In addition the EI Code contains important **record keeping** obligations which are relevant to the processes for handling this material. At Chapter 5 of the EI Code [Vol 1/CM1/p722] there is a checklist of matters which should be centrally retrievable for at least 3 years – as set out at §§60-61 of the Appendix to this skeleton argument.

76. As to **destruction**:

- (a) Chapter 6 of the EI Code [Vol 1/CM1/p723-725] contains provisions about destruction at §6.10 including that information obtained by equipment interference and all copies, extracts and summaries thereof, be marked for deletion and securely destroyed as soon as they are no longer needed to fulfil the Intelligence Services functions. Further if such information is retained it should be reviewed at appropriate intervals to confirm if the justification for its retention is still valid.

- (b) In any event, pursuant the DPA, GCHQ is not exempt from an obligation to comply with the fifth data protection principle, which provides:

“5. Personal data processed²² for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. ...”

Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being used/retained (see the Appendix to this skeleton at §§106-108).

77. In those circumstances, Weber requirements (3)-(6) are also met.

78. It is also to be noted, in terms of substantive safeguards, that GCHQ has a comprehensive programme of training and testing in place for those involved in CNE operations and for intelligence analysts who may have access to data obtained in CNE operations. This training includes operational and mandatory

²² The term “processing” is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

legalities training and the training involves testing and regular re-assessment (see §68C of Ciaran Martin's first witness statement [**Open Bundle/Part B/p139**]).

79. As set out above, when assessing whether there are adequate arrangements in place to give the individual adequate protection against arbitrary interference, both the (1) below the waterline arrangements and (2) oversight mechanisms in the regime are also relevant to the question of Article 8 compliance.
80. The **below the waterline** rules, requirements and arrangements can be appropriately assessed by the Tribunal in CLOSED based on the CLOSED evidence which has been served by the Respondents. It is of note however that, as a result of the disclosure process in these proceedings, some details about these arrangements are now in OPEN, as set out at §§99B-99ZS of the Re-Re-Amended OPEN response and as replicated in §138ff of the Appendix to this skeleton argument. Those rules, requirements and arrangements fully support the contentions set out above about the lawfulness of the regime. Of particular note is the following:
- (a) The provision of internal guidance in the form of the Compliance Guide and both s.5 and s.7 ISA Guidance on the processes for applying, renewing and cancelling warrants/authorisations.
 - (b) Internal safeguards which ensure that decisions to obtain data from implanted devices are lawful, including the provision of training and legal advice.
 - (c) Internal policies for the storage of and access to data, including the setting of maximum limits for storage of operational data. In this regard it is to be noted that all operational data, including that obtained by CNE, is treated as if it was obtained under RIPA.
 - (d) Internal rules regarding the handling/disclosure/sharing of operational data, again which apply as if the material had been obtained under RIPA.
 - (e) Detailed record-keeping arrangements, including processes for keeping all internal Approvals and Additions (see §86B and §71L of Ciaran Martin's first witness statement).
81. As to the **oversight mechanisms** which are relevant to the Article 8(2) compatibility of the regime, the extent of scrutiny of GCHQ's s.5/s.7 ISA operations in this area is of some considerable importance.
82. As is evident from the first witness statement of Ciaran Martin at §§69-73 [**Open Bundle/Part B/pp140-144**] the **Commissioner** plays a very important role in scrutinising the CNE operations of GCHQ. During his visits (both formal and 'under the bonnet') it is apparent that there is a constructive

dialogue between GCHQ and the Commissioner about CNE activities, their authorisation processes and the safeguards which apply to them. These visits have included paying particular attention to the "Additions" layer (under internal approvals) of the s.7 authorisation process and GCHQ's operational use of CNE (see §§71I-71K of Ciaran Martin's first statement).

83. Of particular importance are the Commissioner's conclusions in his 2014 report about GCHQ's record keeping and its s.7 internal approvals process. In particular in his 2014 report he stated:

"GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips." ...

"My under the bonnet inspection in December provided me with a greater understanding of how GCHQ's internal approvals apply to section 7 class authorisations. I was satisfied with the formality of the audit trail and the level of consideration that was given to each operation; it was clear to me that a great deal of thought was going into the process..." ...

... "I wanted to be clear what consideration was being given to protecting privacy at each stage of the process and what was done with any product obtained. I stressed to them the importance I place on filters which help avoid any unnecessary intrusion."

"I was impressed with the formality of the audit trail and the level of consideration; it was clear to me that a great deal of thought was going into assessing the necessity for the activity in the national interest and to ensure privacy was invaded to the least degree possible. In future I recommended that these additions are included in the list of operations provided to me to allow me to select for closer examination and also to ensure I have a full understanding of the scale of operations in GCHQ."

These comments endorse the care and attention which is being given within GCHQ to these processes and the effectiveness of the protections which guard against arbitrary conduct.

84. The ISC specifically considered GCHQ's equipment interference activities as part of its review *"Privacy and Security: A modern and transparent legal framework"* published on 12 March 2015 [Vol 1/CM1/p555ff]. That report, as the Committee made clear in paragraph (v) of the introduction, contained an unprecedented amount of information about the intrusive capabilities used by the UK SIAs. Overall the Committee concluded that the UK SIAs do not seek to circumvent the law, including the requirements of the HRA which governs everything the Agencies do (p2). As is evident from §173-178 of the report this included scrutiny of GCHQ's computer network activities³³ [p621-624].

³³ In terms of the concerns expressed at §177 of the ISC report, the evidence of Ciaran Martin at §71I of his first statement is to be noted i.e. given the Commissioner's clear endorsement of GCHQ's

85. It is submitted that the combination of these oversight mechanisms, including the important oversight provided by this Tribunal, are important safeguards in the context of the Art 8(2) compatibility of the regime.
86. **In conclusion** since February 2015 the Equipment Interference Regime has been sufficiently accessible and “foreseeable” for the purposes of the “in accordance with the law” requirement in Art. 8(2). Article 10 adds nothing to the analysis under Article 8 ECHR – see §147 of *Weber and Saravia v. Germany* (2008) 46 EHRR SE5 [A2/Tab 49] and see also §12 and §149 of the *Liberty/Privacy* judgment [A2/Tab 22].

Compatibility of the regime pre February-2015

87. When considering the compatibility of the regime pre-February 2015 the relevant Code of Practice is the Covert Surveillance and Property Interference Code (“the Property Code”) as addressed in detail at §§76-100 of the Appendix to this skeleton argument. This was first issued in 2002 (called the Covert Surveillance Code of Practice) and was then revised in September 2010 with further revisions in 2014. As explained in the Appendix to this skeleton, there were no material differences between the 2010 and 2014 versions of the Property Code in terms of property interference.

Weber (1) and (2)

88. The Respondent repeats those submissions at §§63-65 above regarding these requirements. These requirements i.e. the “offences” which may give rise to a warrant/authorisation and the categories of people liable to be involved, are clearly satisfied by s. 5 and s.7 of the ISA, as read, in particular, with Chapter 3 and 7 of the 2010/2014 Property Code and Chapter 2 and 6 of the 2002 Property Code.
89. In the 2010/2014 version of the Property Code [Vol 1/CM1/p734ff]:
- (a) Chapter 7 set out the authorisation processes for property interference including a checklist of matters about which the Secretary of State had to be satisfied/consider before issuing a warrant/authorisation including at §7.38 [p809]:
 - i. being satisfied that it is necessary for the purposes of carrying out the intelligence services functions;

internal record keeping, including its s.7 processes, he does not consider that the statement relates to GCHQ’s s.7 ISA operations.

- ii. being satisfied that it is proportionate;
 - iii. taking into account whether there are other means by which the information could reasonably be obtained; and
 - iv. being satisfied that there are satisfactory arrangements in place as regards disclosure of any information obtained.
- (b) In addition it was made clear in §7.37 [p809] that the intelligence services should provide the same information as other agencies, as and where appropriate, when making applications for the grant or renewal of property warrants. That in turn meant that the checklist at §7.18 [p804] setting out the information which should be specified in applications should be provided where possible i.e.
- *“the identity or identities, where known, of those who possess the property that is to be subject to the interference;*
 - *sufficient information to identify the property which the entry or interference with will affect;*
 - *the nature and extent of the proposed interference;*
 - *the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;*
 - *details of the offence suspected or committed;*
 - *how the authorisation criteria (as set out above) have been met;*
 - *any action which may be necessary to maintain any equipment, including replacing it;*
 - *any action which may be necessary to retrieve any equipment;*
 - *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and*
 - *whether an authorisation was given or refused, by whom and the time and date on which this happened.”*
- (c) Chapter 3 set out general rules on authorisations, including guidance on the requirements of proportionality at §§3.3-3.6 including specific elements of proportionality that should be considered at §3.6 (see §80 of the Appendix to this skeleton argument and [Vol 1/CMI/p760]);
- (d) Guidance on collateral intrusion was also given in that Chapter at §§3.8-3.11 (see §83 of the Appendix [Vol 1/CMI/p761-762]);
- (e) Best working practice guidance was also given at §§3.27-3.28 ([Vol 1/CMI/p766-767] NB. §§3.28-3.29 in the 2014 version) including making sure that there is a designated senior official within each of the Intelligence Services responsible for, *inter alia*, the integrity of the process to authorise equipment interference and engagement with the Commissioner.

90. In the 2002 Property Code similar provisions were to be found, in particular, in Chapter 2 and Chapter 6 – see §§93-99 of the Appendix to this skeleton argument, including an alternative version of the checklist of information to be

specified in applications at §6.12 of the Code.

91. In the light of the matters set out above it is submitted that the pre-February 2015 regime is sufficiently clear both as to the nature of the offences which may give rise to equipment interference activity and the categories of person liable to be subject to such measures.

Weber (3)-(6)

92. The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are addressed, in particular, in the ISA, the CTA, the DPA, the HRA, the OSA and in Chapters 7-9 of the 2010/2014 Property Code and Chapter 6 of the 2002 Property Code and GCHQ's internal arrangements. In particular:

93. In terms of **duration**:

- (a) The ISA makes sufficient provision for the duration of s.5/s.7 warrants/authorisations and the circumstances in which they can be renewed or should be cancelled – see s.6 and s.7(5)-7(7) of the ISA (referred to at §§23-26 and 33-35 of the Appendix to this skeleton, [A1/Tab 7]).
- (b) In addition the Property Code contains important provisions on renewals and cancellations:
- i. In the 2010/2014 Property Code these are contained in §§7.39-7.42 (see §86 of the Appendix to this skeleton and [Vol 1/CM1/p810]); and
 - ii. In the 2002 Property Code these are contained in §§6.34-6.35 (see §97 of the Appendix).

It is to be noted that in *RE v United Kingdom* the provisions in Part II of RIPA and in the Revised Property Code (i.e. issued in 2010) were considered to be "sufficiently clear" see §137 [A2/Tab 44].

94. As regards the **handling, dissemination, copying, storage, disclosure and security arrangements** for information obtained as a result of equipment interference.

- (a) Pursuant to the 2010/2014 Property Code, guidance is given as to the handling of material obtained through property interference. §9.3 of the Code [Vol 1/CM1/p814] addresses the retention and destruction of material and stated as follows:

“Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.” (emphasis added)

In addition the Code states at §9.7 [p815] that, in relation to the Intelligence Services:

“The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the ... 1994 Act.” (emphasis added)

In the 2002 version of the Code, the same provision as §9.7 above was set out at §2.19.

- (b) Any information emanating from equipment interference can be used by GCHQ only in accordance with s.19(2) of the CTA as read with the statutory definition of GCHQ’s functions (in s. 3 of the ISA) and only insofar as proportionate under s.6(1) of the HRA.
- (c) Pursuant the DPA, GCHQ is not exempt from an obligation to comply with the seventh data protection principle, which provides:

*“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”*³⁴

Accordingly, as set out earlier in these submissions, if GCHQ obtain any information as a result of any property interference which amounted to personal data, it is obliged to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question (see the Appendix to this skeleton at §§106-108.

- (d) Any disclosure eg. deliberately in breach of the “arrangements” for which provision is made in s.4(2)(a) of the ISA would be a criminal

³⁴ The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

offence under s.1(1) of the OSA which could attract imprisonment of up to two years (see the Appendix to this skeleton at §109).

- (e) Further a member of the intelligence service will commit an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the ISA read with s.1(1)). Conviction may lead to imprisonment of up to 3 months (see the Appendix to this skeleton at §110).
- (f) Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 at §§191-194).
- (g) Finally any disclosure of such information had to satisfy the constraints imposed in s. 3-4 of the ISA, as read with s.19(5) of the CTA and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

95. As to **destruction**:

- (a) The 2010/2014 Property Code address the destruction of material at §9.3 [Vol 1/CMI/p814] and states as follows :

*“Each public authority must ensure that arrangements are in place for the secure handling, storage and **destruction** of material obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.”* (emphasis added)

In addition the Code states at §9.7 [p815] that, in relation to the Intelligence Services:

“The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions...” (emphasis added)

- (b) In the 2002 version of the Code, the same provision as §9.7 above was set out at §2.19.

- (c) Pursuant the DPA, GCHQ is not exempt from an obligation to comply with the fifth data protection principle, which provides:

“Personal data processed³⁵ for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

...”

Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained/used (see the Appendix to this skeleton at §§106-108).

96. In those circumstances, the *Weber* requirements (3)-(6) are also met for the pre-February 2015 regime.
97. In addition, those substantive safeguards set out at 78 to 85 above including the below the waterline arrangements and the oversight mechanisms, are highly relevant to the Article 8 compatibility of the pre-February 2015 regime. Those submissions are not repeated, but are of relevance when considering “all the circumstances” and whether overall the pre-February 2015 regime contained effective safeguards against abuse.
98. Whilst it is accepted that pre-February 2015 regime does not contain some of the detail to be found in the EI Code (eg. in Chapter 6), it is submitted that, in all the circumstances of the case, and particularly given the safeguards and the supervision regime which were in place throughout, it was “in accordance with the law” pursuant to Article 8 ECHR.

Proportionality

99. For reasons discussed earlier in this skeleton argument, there are considerable limits on GCHQ’s ability to address in OPEN the matters which are relevant to an assessment of the proportionality of GCHQ’s activities. However the following brief OPEN submissions are made at this stage:

- (a) As made clear eg. in *Leander v Sweden*, in the field of national security the state has a wide margin of appreciation in assessing the pressing social need and in choosing the means for achieving the legitimate aim of protecting national security (see **A2/Tab 40/§§58-59** and see also the Tribunal’s conclusions in *Liberty/Privacy* at §§38-39 [**A2/Tab**

³⁵ The term “processing” is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

22])).

- (b) As explained in Ciaran Martin's first witness statement at §§6-20 and 28-34 [**Open Bundle/Part B/pp125-129, 130-131**] the terrorist threat currently facing the UK is SEVERE and GCHQ's CNE activity is increasingly required to enable the UK to counter that threat. The fact that CNE may, in some cases, be the only way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country is of obvious importance to the proportionality assessment (see §31 of Ciaran Martin's first statement).
- (c) As already made clear, the Claimants' extreme allegations about the size, scope and intrusiveness of GCHQ's CNE activity must be contrasted with the reality of GCHQ's operations, as have been explained in detail in the CLOSED evidence.

100. It is therefore submitted that GCHQ's CNE activities are proportionate and have been throughout the relevant period since 1 August 2009.

Specific questions posed in the list of issues

101. A number of specific questions have been posed in the list of issues at §5. Some of the answers to these questions follow from and are answered by the submissions above. However, in summary, the Respondents' answers to these questions is as follows:
- a. *Should CNE activities be authorised by specific and individual warrants, or is it sufficient that they be authorised by 'class' or 'thematic' warrants or authorisations without reference to a specific individual target?*
102. Section 5 ISA activity is authorised by specific warrants and submissions about the compatibility of descriptive warrants with s.5 ISA have already been addressed under Issue 2 above.
103. Section 7 authorisations can relate to a broader class of operations, as made clear in s.7 of the ISA and at §7.6 of the EI Code. Further there is nothing in the case law under Article 8 ECHR which precludes this, particularly given that the regime satisfies the minimum *Weber* requirements for the reasons set out in detail above.
104. In this regard it is relevant that *Weber* itself concerned a regime known as "strategic monitoring" which did not involve interception that had to be targeted at a specific individual or premises (see §§110-111 [**A2/Tab 49**]). Despite that, the applicants' Art. 8 challenge in *Weber* to strategic monitoring

was not merely rejected, it was found to be “manifestly ill-founded” (§§137-138) and thus inadmissible. In the s.7 ISA context, whilst the authorisation may relate to a broad class of operations and may not be narrowed to a specific target in the first instance, there are then detailed procedures in place, both above and below the waterline, to ensure that operations pursuant to that authorisation meet the same stringent tests as would be required for a s.5 ISA warrant (see §7.13 of the EI Code [Vol 1/CM1/p728]).

105. Consequently the procedures for s.7 authorisations are entirely compatible with Article 8 ECHR.

b. What records ought to be kept of CNE activity? Is it necessary that records of CNE activity are kept that record the extent of the specific activity and the specific justification for that activity on grounds of necessity and proportionality, identifying and justifying the intrusive conduct taking place?

106. The EI Code makes provision for the records which should be kept of CNE activity (see Chapter 5 of the EI Code [Vol 1/CM1/p722]). In addition GCHQ’s own processes include maintaining indefinitely records of the application for, renewal of, approval of and cancellation of all warrants under s.5 and class authorisations and internal approvals under s.7. These include comments or stipulations from the Secretary of State relating to them (see §68B of Ciaran Martin’s first statement [Open Bundle/Part B/p139]). By definition, that means that the specific justification for the activity in question in terms of necessity and proportionality will be included as part of the record keeping.

107. The Respondents accept that such records should be kept and would emphasise the extent to which the Commissioner has commended GCHQ’s compliance in this regard; stating in his 2014 report:

“GCHQ also take compliance extremely seriously and the paperwork GCHQ provided was in good order and I found no slips.” ...

“I was impressed with the formality of the audit trail...” [Open Bundle/Part B/§72C/pp143-144]

d. What, if any, is the relevance of the fact that, until February 2015, it was neither confirmed nor denied that the Respondents carried out CNE activities at all?

108. In circumstances where the statutory regime has provided for property

interference by GCHQ in compliance with its statutory functions³⁶ since the introduction of the ISA 1994, it is not accepted that it is of any relevance that GCHQ did not admit to carrying out CNE activity until February 2015.

109. It is well understood by the Tribunal that national security considerations mean that much less is required to be put into the public domain (see *Liberty/Privacy* at §§38-39). Inevitably therefore there will be a tension between the development by eg. GCHQ of innovative technologies/techniques for property interference which national security considerations require to be kept secret and the extent to which such technologies/techniques can be addressed publicly. The fact that it was neither confirmed nor denied that GCHQ actually carried out such activities until February 2015 does not undermine the legality of the regime in circumstances where the statutory powers and functions of GCHQ could reasonably have been taken to include interference with computer equipment prior to that time.

e. What, if any, is the relevance of the Covert Surveillance and Property Interference Code, issued in 2002 and updated in 2010 and 2014?

110. As set out above, the Property Code is of particular relevance to the compatibility of the equipment interference regime with Article 8 ECHR prior to February 2015.

f. What, if any, is the effect of the publication of a Draft Equipment Interference Code of Practice in February 2015?

111. For reasons set out above, the draft Code provides more detailed provisions, but does not affect the Article 8 compliance of the regime given that the pre-February 2015 regime was also ECHR compliant.

g. What, if any, is the relevance of the Intelligence Services Commissioner's oversight of the use of the powers contained within ISA 1994?

112. The oversight provided by the Commissioner is a very important safeguard when assessing the overall ECHR compatibility of the regime for reasons already set out in detail above.

h. What, if any, is the relevance of the oversight by the Tribunal and the Intelligence and Security Committee of Parliament?

³⁶ GCHQ's statutory functions include "... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material".

113. The oversight provided by the ISC is also a very important safeguard when assessing the overall ECHR compatibility of the regime for reasons already set out in detail above.

LPP and Confidential Information

c. Have adequate safeguards been in place at all times to prevent the obtaining, storing, analysis or use of legally privileged material and other sensitive confidential documents?

114. In terms of the regime for the handling of legally privileged material, the Respondents accepted in the Belhaj IPT proceedings recorded in the Tribunal's Order dated 26 February 2015 namely that, "since January 2010 the regime for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material has contravened Article 8 ECHR and was accordingly unlawful". Consistently with that, insofar as LPP material was obtained, analysed etc. it is accepted that the regime was unlawful in this earlier period.
115. The only issue that the Claimants have identified under this heading in these proceedings about the compatibility of the regime since February 2015 relates to the LPP provisions in respect of communications data. After being invited to clarify their case, the Claimants stated as follows³⁷:

"The regime subsequent to the publication of the draft EI Code is not prescribed by law, because (in error of law) the draft Code does not recognise that communications data may be protected by LPP. These arguments will be familiar to the Tribunal and the Respondents. They were run by the Law Society in Belhaj (albeit it was not necessary for them to be ruled on in that case), and considered by the Divisional Court in R (Davis & Watson) v SSHD [2015] EWHC 2092 (Admin). Indeed, many of the same counsel were instructed in these cases."

116. The Respondents do not accept that there is any error of law in the EI Code as contended for by the Claimants.
- (a) The language which is used in the EI Code is not the same as that used in the Acquisition of Communications Data Code of Practice at §3.72ff³⁸. In particular the EI Code refers in Chapter 3 to "knowledge

³⁷ see Bhatt Murphy's email of 12 November 2015 at 19:15.

³⁸ That Code states as follows:

3.72. Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.

of matters subject to legal privilege” eg. in §3.6 [Vol 1/CM1/p715]. It does not contain any absolute statement that communications data is not subject to any form of professional privilege, in contrast to §3.72 of the Acquisition of Communications Data Code.

- (b) In any event and without prejudice to that, the Divisional Court in *Davis and Watson* did not find the Acquisition of Communications Data Code to be unlawful in this regard, given the rare circumstances in which communications data might engage LPP and the protections which were in fact in place in the later provisions of that Code. Consequently at §§67-68 the Divisional Court stated:

*“67. The Code of Practice issued by the Secretary of State states that communication data will not be subject to legal professional privilege since there will be no access to the contents of retained communications. The Law Society made written submissions which challenge the correctness of this statement. Reliance is placed on a dictum of Cotton LJ in *Gardner v. Irvin* (1878) 4 Ex D 49 at 83 where he said:-*

“I think that the plaintiffs are not entitled to have the dates of the letters and such other particulars of the correspondence as may enable them to discover indirectly the contents of the letters, and thus to cause the defendants to furnish evidence against themselves in this action”.

*This approach was confirmed by Vinelott J in *Derby v. Weldon* (No 7) [1990] 1 WLR 1156.*

68. No doubt such an example of privilege would rarely arise. However, communications with practising lawyers do need special

3.73. However the degree of interference with an individual’s rights and freedoms may be higher where the communications data being sought relates to a person who is a member of a profession that handles privileged or otherwise confidential information (including medical doctors, lawyers, journalists, Members of Parliament,⁹⁴ or ministers of religion). It may also be possible to infer an issue of sensitivity from the fact someone has regular contact with, for example, a lawyer or journalist.

3.74. Such situations do not preclude an application being made. However applicants, giving special consideration to necessity and proportionality, must draw attention to any such circumstances that might lead to an unusual degree of intrusion or infringement of rights and freedoms, particularly regarding privacy and, where it might be engaged, freedom of expression. Particular care must be taken by designated persons when considering such applications, including additional consideration of whether there might be unintended consequences of such applications and whether the public interest is best served by the application.

3.75. Applicants must clearly note in all cases when an application is made for the communications data of those known to be in such professions, including medical doctors, lawyers, journalists, Members of Parliament, or ministers of religion. That such an application has been made must be recorded (see section 6 on keeping of records for more details), including recording the profession, and, at the next inspection, such applications should be flagged to the Interception of Communications Commissioner.

consideration. The same in our view can properly be said to apply to communications with MPs. The Code of Practice makes clear the need for such special attention." (emphasis added)

25 November 2015

JAMES EADIE QC
DANIEL BEARD QC
KATE GRANGE
RICHARD O'BRIEN

APPENDIX

THE EQUIPMENT INTERFERENCE REGIME

1. The Equipment Interference Regime which is relevant to the activities of GCHQ principally derives from the following statutes:
 - (a) the Intelligence Services Act 1994 ("the ISA"), (as read with the Counter-Terrorism Act 2008 ("the CTA") and the Computer Misuse Act 1990 ("the CMA"));
 - (b) the Human Rights Act 1998 ("the HRA");
 - (c) the Data Protection Act 1998 ("the DPA"); and
 - (d) the Official Secrets Act 1989 ("the OSA").
2. In addition, the draft Equipment Interference Code of Practice dated February 2015 ('the EI Code') and the Covert Surveillance and Property Interference Code of Practice 2002 ('the Property Code')¹ are relevant to the regime as regards the scope of any powers to interfere with property and equipment.
3. There are also important **oversight mechanisms** in the regime provided by the Intelligence Services Commissioner, the Intelligence and Security Committee and the Tribunal.
4. In addition and in accordance with the Codes, GCHQ has a number of **internal arrangements** in relation to CNE activities; an open summary of which appears at the end of this Appendix.

The ISA (read with the CTA and the CMA)

GCHQ functions

5. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ..."
6. By s. 3(2) of the ISA, these functions are only exercisable:
 - "(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
 - (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
 - (c) in support of the prevention or detection of serious crime."*
7. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

"... that there are arrangements for securing that no information is obtained by GCHQ

¹ The Property Code was first issued in 2002 and further versions of the Code were published in 2010 and on 10 December 2014 (in terms of property interference there is no material difference between the 2010 and the 2014 versions of the Code).

except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

Disclosure of information

8. By s. 19(5) of the CTA, information obtained by GCHQ for the purposes of any of its functions *"may be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings."*

9. Thus, specific statutory limits are imposed on the information that GCHQ can obtain, and on the information that it can disclose. In addition, the term "information" is a very broad one, and is capable of covering e.g. both communications and communications data.

10. By s. 19(2) of the CTA:

"Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions."

Computer Misuse Act ('CMA')

11. The Computer Misuse Act 1990 (CMA) came into force on 29 June 1990. It was amended on 3 May 2015 as a result of changes introduced by the Serious Crime Act 2015.

12. By s.1(1) of the CMA:

*"(1) A person is guilty of an offence if—
(a) he causes a computer to perform any function with intent to secure access to any program or data² held in any computer;*

² Section 17 of the CMA provides, *inter alia*, that:

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

- (a) alters or erases the program or data;*
- (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;*
- (c) uses it; or*
- (d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);*

and references to access to a program or data (and to an intent to secure such access [or to enable such access to be secured] 1) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform—

- (a) causes the program to be executed; or*
- (b) is itself a function of the program.*

(4) For the purposes of subsection (2)(d) above—

- (a) a program is output if the instructions of which it consists are output; and*
- (b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial. ...*

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(b) the access he intends to secure, is unauthorised³; and
(c) he knows at the time when he causes the computer to perform the function that that is the case.”

13. Although “computer” is not defined in the CMA, in the context of s.69 of the Police and Criminal Evidence Act 1984 (PACE), the term has been held to mean “a device for storing, processing and retrieving information” (see *DPP v McKeown* [1997] 1 WLR 295 at 302).
14. By s.3 of the CMA it is also an offence to do any unauthorised act⁴ in relation to a computer, if, at the time that he does the act the person knows that it is unauthorised (s. 3(1)) and either (1) the intention is to impair the operation of any computer; to prevent or hinder access to any program or data held in any computer; to impair the operation of any such program or the reliability of any such data (s. 3(2)(a)-(c)), or (2) the person is reckless as to whether the act will do any of those things s. 3(3).
15. Section 4 of the CMA sets out the territorial scope of, *inter alia*, offences under s. 1 and s. 3 of the CMA. In particular this makes clear that it is immaterial for the purposes of any offence under s.1 or s.3 of the CMA (a) whether any act or other event, proof of which is required for conviction of the offence, occurred in England or Wales; or (b) whether the accused was in England or Wales at the time of any such act or event. Save in respect of certain offences (i.e. under s. 2 of the CMA), at least one significant link with domestic jurisdiction must exist in the circumstances of the case for an offence to be committed. The tests as to whether there is a significant link with domestic jurisdiction are set out in section 5 of the CMA.
16. Summary conviction under the CMA in respect of offences under s. 1 and s. 3 may lead to imprisonment for a term not exceeding 12 months or a fine (see s. 1(3)(a) and s. 3(6)(a) CMA). Any conviction on indictment may lead to imprisonment for a term not exceeding 2 years or to a fine, or both, in respect of a s. 1 offence (see s. 1(3)(c)) and for a term not exceeding 10 years, or to a fine, or both in respect of a s. 3 offence (see s. 3(6)(c) CMA).
17. Section 10 of the CMA (prior to amendments introduced on 3 May 2015) provided as follows:

*“Saving for certain law enforcement powers
Section 1(1) above has effect without prejudice to the operation –
(a) In England and Wales of any enactment relating to powers of inspection, search or seizure.”*
18. On 3 May 2015 the CMA was amended. Those amendments (which it is accepted are not retrospective) included, *inter alia*:
 - a) Changes to the test under section 5 as to when a significant link with domestic

³ By section 17(5) of the CMA – “Access of any kind by any person to any program or data held in a computer is unauthorised if— (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled” (NB. this subsection is subject to section 10 which contains a saving in respect of certain law enforcement powers).

⁴ By s. 17(8) of the CMA - An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)— (a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and (b) does not have consent to the act from any such person. In this subsection “act” includes a series of acts.

jurisdiction is established in respect of offences under, *inter alia*, sections 1 and 3 of the CMA;

- b) Changes to section 10 of the CMA, which now provides *inter alia*:

“Savings

Sections 1 to 3A have effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required...” (changes underlined)

Authorisation for equipment interference

s.5. warrants

19. By s. 5 of the ISA the Intelligence Services, including GCHQ, can apply for a warrant which provides specific legal authorisation for property interferences by them. Thus by s5(1) of the ISA:

“(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.

20. In relation to GCHQ, pursuant to s.5(2)(a)-(c) of the ISA the Secretary of State can only issue a warrant under s.5 following an application by GCHQ if he/she is satisfied that:

- (a) it is **necessary** for the action to be taken for the purpose of assisting GCHQ in carrying out its statutory functions under s. 3(1)(a) of the ISA;
- (b) the taking of the action is **proportionate** to what the action seeks to achieve; and
- (c) **satisfactory arrangements** are in force under section 4(2)(a) of the ISA with respect to the disclosure of information by GCHQ obtained by virtue of the section and any information obtained under the warrant will be subject to those arrangements.

21. When exercising his/her discretion and considering necessity and proportionality, the Secretary of State must take into account *“whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means”* (s.5(2A) ISA).

22. Pursuant to s. 5(3) of the ISA GCHQ may not be granted a s.5 warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

23. By s.6 of the ISA the procedure for issuing warrants and the duration of s. 5 warrants is addressed. In particular s.6(1) provides that a warrant shall not be issued save under the hand of the Secretary of State, unless it is a species of urgent case as set out in s.6(1)(b) or (d)⁵.

24. In terms of duration, unless the warrant is renewed, it ceases to have effect at the end of the period of six months, beginning with the day on which it was issued (s. 6(2)) (save where the warrant was issued urgently and not under the hand of the Secretary of State in which case it

⁵ Those sub-sections provide:

(b) in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed on it, under the hand of a senior official; ...

(d) in an urgent case where the Secretary of State has expressly authorised the issue of warrants in accordance with this paragraph by specified senior officials and a statement of that fact is endorsed on the warrant, under the hand of any of the specified officials.

lasts for 5 working days).

25. As to renewal, under s.6(3) of the ISA, if, before the expiry of the warrant, the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, it may be renewed for a period of six months.
26. By s. 6(4) of the ISA "*The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary*".

s.7 authorisations

27. In terms only of acts outside the British Islands, s.7 of the ISA also provides for the authorisation of such acts by the Intelligence Services including GCHQ. S.7(1) and 7(2) provide:

"(1) If, apart from this section; a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.

(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom."

28. Acts outside the British Islands include cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus (s. 7(9) ISA).⁶
29. However, pursuant to s.7(3) of the ISA, the Secretary of State shall not give an authorisation under s. 7 of the ISA to GCHQ unless he/she is satisfied:

"(a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a function of GCHQ; and

(b) that there are satisfactory arrangements in force to secure—

(i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of ...GCHQ; and

(ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and

(c) that there are satisfactory arrangements in force under section... 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

30. Under s. 7(4) of the ISA such an authorisation by the Secretary of State:

⁶ In addition ss.7(10)-(14) of the ISA recognise that it may be difficult, in certain circumstances to ascertain reliably the location of property and therefore provide, *inter alia*, that where acts are done in relation to property which is eg. mistakenly believed to be outside the British Islands, but which is done before the end of the 5th working day on which the presence of the property in the British Isles first becomes known, those acts will be treated as done outside the British Islands.

“(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;

(b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified.”

31. Consequently the type of acts which may be covered by a s. 7 authorisation are broadly defined in the ISA and can clearly cover equipment interference outside the British Islands, where the tests in s. 7(3) of the ISA are satisfied.
32. By s. 7(5) of the ISA, an authorisation shall not be given except under the hand of the Secretary of State, or in an urgent case and where the Secretary of State has expressly authorised it to be given under the hand of a senior official.
33. In terms of duration, unless it is renewed, a s. 7 authorisation ceases to have effect at the end of the period of six months beginning on the day on which it was given (save if it was not given under the hand of the Secretary of State in which case it lasts for 5 working days) (see s. 7(6) ISA).
34. Pursuant to s. 7(7) the authorisation can be renewed for a period of six months, if the Secretary of State considers it necessary to continue to have effect for the purpose for which it was given.
35. By s. 7(8) of the ISA *“The Secretary of State shall cancel an authorisation if he is satisfied that the action authorised by it is no longer necessary”*.
36. Consequently both s. 5 warrants and s.7 authorisations provide the Intelligence Services, including GCHQ, with specific legal authorisation for equipment interference, with the effect that the Intelligence Services are not civilly or criminally liable for such interferences, including under the CMA.

The Equipment Interference Code of Practice (‘the EI Code’)

37. The draft Equipment Interference Code of Practice (‘the EI Code’) was published on 6 February 2015 by the Home Office. It was issued pursuant to section 71 of RIPA⁷ and was subject to public consultation between 6 February 2015 and 20 March 2015 in accordance with s. 71(3) of RIPA. On 4 November 2015 an amended version of the Code was laid before both Houses of Parliament and must now be the subject to affirmative resolution by both Houses (see draft ‘The Equipment Interference (Code of Practice) Order 2015’).
38. However, as set out in the Written Ministerial Statement which accompanied the publication of the draft Code in February 2015, the safeguards in that Code reflected the safeguards

⁷ S. 71 of RIPA imposes a duty on the Secretary of State to issue, following appropriate consultation, one or more codes of practice relating to the exercise and performance of the powers and duties conferred or imposed by or under, *inter alia*, section 5 of the Intelligence Services Act 1994. Any person exercising or performing any power or duty in relation to which provision may be made by a code of practice under section 71, must have regard to any relevant provisions of every code of practice for the time being in force: s. 72(1). Further, where the provision of a code of practice appears to the Tribunal, a court or any other tribunal to be relevant to any question arising in the proceedings, in relation to a time when it was in force, that provision of the code must be taken account in determining that question. A similar duty is imposed on the Commissioner: see s. 72(4) of RIPA. The code of practice can be taken into account in assessing “foreseeability” for the purposes of Art. 8(2): *Kennedy v United Kingdom* (2011) 52 EHRR 4, at §157.

applied by the relevant Agencies, including GCHQ. GCHQ can confirm that it complies with all aspects of the EI Code and can also confirm that it fully reflects the practices, procedures and safeguards which GCHQ has always applied to any equipment interference activities carried out by it.

39. As to the differences between the draft Code dated 6 February 2015 and the Code as recently laid before Parliament in November 2015, the two changes of substance are as follows:
- (a) In Chapter 3 dealing with Legally Privileged and Confidential Information there are some changes to §§3.4 to 3.14 including, *inter alia*, new text in 3.4 and 3.11-3.12 and changes in 3.6-3.10 as compared with 3.5-3.8 of the draft Code. There is also a change to the last sentence of §3.25 and 3.28 is new text.
 - (b) In Chapter 5 dealing with record keeping, three new bullets have been added (bullets 1, 3 and 4) as they appear at §5.1 so that there are more detailed requirements for record-keeping.
40. Otherwise there have been minor tweaks to the language of the Code, for example, in §§1.7, 6.5, 6.11, 7.1, 7.2, 7.12, 7.13, 7.14 and 7.6 the word "should" now appears instead of the word "must".
41. The EI Code provides guidance on the use by the Intelligence Services of s. 5 and s.7 of the ISA to authorise equipment interference to which those sections apply. In particular it provides guidance on the procedures that must be followed before equipment interference can take place, and on the processing, retention, destruction and disclosure of any information obtained by means of the interference.
42. To the extent that the EI Code overlaps with the guidance provided in the Covert Surveillance and Property Interference Revised Code of Practice issued in 2014 (see further below), the EI Code takes precedence, however the Intelligence Services must continue to comply with the 2014 Code in all other respects (see §1.2).
43. The EI Code also records the fact that there is a duty on the heads of the Intelligence Services to ensure that *arrangements* are in force to secure: (i) that no information is obtained by the Intelligence Services except so far as necessary for the proper discharge of their statutory functions; and (ii) that no information is disclosed except so far as is necessary for those functions (see §1.3 of the EI Code and the statutory framework under the ISA set out above).

Equipment interference to which the EI Code applies

44. The EI Code identifies specific types of equipment interference to which the code applies. At §1.6 it states:

"This code applies to (i) any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, and (ii) information derived from any such interference, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:

- a) obtain information from the equipment in pursuit of intelligence requirements;*
- b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;*
- c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);*
- d) enable and facilitate surveillance activity by means of the equipment.*

“Information” may include communications content, and communications data as defined in section 21 of the 2000 Act.”

45. At §1.7 of the EI Code it summarises the effect of a s.5 warrant and states:

“The section 5 warrant process must [should^f] be complied with in order properly and effectively to deal with any risk of civil or criminal liability arising from the interferences with equipment specified at sub-paragraphs (a) to (d) of paragraph 1.6 above. A section 5 warrant provides the Intelligence Services with specific legal authorisation removing criminal and civil liability arising from any such interferences.”

Basis for lawful equipment interference activity

46. In addition to highlighting the statutory functions of each Intelligence Agency, the EI Code specifically draws attention to the HRA and the need to act proportionately so that equipment interference is compatible with ECHR rights. At §§1.10-1.13 the EI Code states:

“1.10 The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, while others are qualified, which means that it is permissible for public authorities to interfere with those rights if certain conditions are satisfied.

1.11 Amongst the qualified rights is a person’s right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when the Intelligence Services seek to obtain personal information about a person by means of equipment interference. Such conduct may also engage Article 1 of the First Protocol (right to peaceful enjoyment of possessions).

1.12 By section 6(1) of the 1998 Act, it is unlawful for a public authority to act in a way which is incompatible with a Convention right. Each of the Intelligence Services is a public authority for this purpose. When undertaking any activity that interferes with ECHR rights, the Intelligence Services must therefore (among other things) act proportionately. Section 5 of the 1994 Act provides a statutory framework under which equipment interference can be authorised and conducted compatibly with ECHR rights.

1.13 So far as any information obtained by means of an equipment interference warrant is concerned, the heads of each of the Intelligence Services must also ensure that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of the disclosure of that information, and that any information obtained under the warrant will be subject to those arrangements. Compliance with these arrangements will ensure that the Intelligence Services remain within the law and properly discharge their functions.”

General rules on warrants

47. Chapter 2 of the EI Code contains a number of general rules on warrants issued under s. 5 of the ISA.

^f “should” now appears in the November 2015 version of the Code and the same point is highlighted by the use of square brackets below.

Necessity and proportionality

48. Within Chapter 2 the EI Code contains detailed guidance on the requirements of necessity and proportionality and how these statutory requirements are to be applied in the EI context. At §§2.6-2.8 it states:

“2.6 Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

2.7 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed interference against what is sought to be achieved;*
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
- evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented.*

2.8 It is important that all those involved in undertaking equipment interference operations under the 1994 Act are fully aware of the extent and limits of the action that may be taken under the warrant in question.”

49. Consequently the EI Code draws specific attention to the need to balance the seriousness of the intrusion against the need for the activity in operational and investigative terms, including taking into account the effect on the privacy of any other person who may be affected i.e. other than the subject of the operation. The EI Code is also very clear that it is important to consider all reasonable alternatives and to evidence what other methods were considered and why they were not implemented.

Collateral intrusion

50. The EI Code also highlights the risks of collateral intrusion involved in equipment interference and provides guidance on how any such issues should be approached, including the need to carry out an assessment of the risk of collateral intrusion. At §§2.9-2.12 it states:

“2.9 Any application for a section 5 warrant should also take into account the risk of obtaining private information about persons who are not subjects of the equipment interference activity (collateral intrusion).

2.10 Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the equipment interference activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

2.11 *All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the Secretary of State fully to consider the proportionality of the proposed actions.*"

51. In addition the EI Code makes clear at §2.12 that where it is proposed to conduct equipment interference activity specifically against individuals who are not intelligence targets in their own right, interference with the equipment of such individuals should not be considered as collateral intrusion but rather as "intended intrusion" and that:

"Any such equipment interference activity should be carefully considered against the necessity and proportionality criteria as described above."

Reviewing warrants

52. At §§2.13-2.15 the Code sets out certain requirements for reviewing warrants and states as follows:

"2.13 Regular reviews of all warrants should be undertaken to assess the need for the equipment interference activity to continue. The results of a review should be retained for at least three years (see Chapter 5). Particular attention should be given to the need to review warrants frequently where the equipment interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

2.14 In each case, unless specified by the Secretary of State, the frequency of reviews should be determined by the member of the Intelligence Services who made the application. This should be as frequently as is considered necessary and practicable.

2.15 In the event that there are any significant and substantive changes to the nature of the interference and/or the identity of the equipment during the currency of the warrant, the Intelligence Services should consider whether it is necessary to apply for a fresh section 5 warrant."

General best practices

53. The EI Code gives guidance on general best practice to be followed by the Intelligence Services when making applications for warrants covered by the Code. At §2.16 those requirements are:

- applications should avoid any repetition of information;*
- information contained in applications should be limited to that required by the 1994 Act;*
- where warrants are issued under urgency procedures (see Chapter 4), a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the applicant and authorising officer as a priority. There is then no requirement subsequently to submit a full written application;*
- where it is foreseen that other agencies will be involved in carrying out the operation, these agencies should be detailed in the application; and*
- warrants should not generally be sought for activities already authorised following an application by the same or a different public authority."*

54. In addition, the EI Code indicates that it is considered good practice that within each of the Intelligence Services, a designated senior official should be responsible for:

- *the integrity of the process in place within the Intelligence Service to authorise equipment interference;*
- *compliance with the 1994 Act and this code;*
- *engagement with the Intelligence Services Commissioner when he conducts his inspections; and*
- *where necessary, overseeing the implementation of any post inspection action plans recommended or approved by the Commissioner.” (see §2.17)*

Legally privileged and confidential information

55. Chapter 3 of the Code contains detailed provisions on legally privileged and confidential information which it is intended to obtain or which may have been obtained through equipment interference.

Procedures for authorising equipment interference under s. 5

56. Chapter 4 of the EI Code sets out the general procedures to be followed for authorising equipment interference activity under s. 5 of the ISA. In that Chapter, §§4.1-4.4 outline the statutory scheme under the ISA. At §4.5 of the code, attention is drawn to the need to consider whether the equipment interference operation might also enable or facilitate a separate covert surveillance operation, in which case a directed or intrusive surveillance authorisation might need to be obtained under Part 2 of RIPA (as addressed in the Covert Surveillance and Property Interference Code).

57. In terms of applications for a s. 5 warrant, the EI Code contains a checklist of the information which each issue or renewal application should contain. At §4.6 it states:

“An application for the issue or renewal of a section 5 warrant is made to the Secretary of State. Each application should contain the following information:

- *the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference;*
- *sufficient information to identify the equipment which will be affected by the interference;*
- *the nature and extent of the proposed interference, including any interference with information derived from or related to the equipment;*
- *what the operation is expected to deliver and why it could not be obtained by other less intrusive means;*
- *details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected.*
- *whether confidential or legally privileged material may be obtained. If the equipment interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege or confidential personal information, but it is likely that such knowledge will nevertheless be acquired during the operation, the application should identify all steps which will be taken to mitigate the risk of acquiring it;*
- *details of any offence suspected or committed where relevant;*
- *how the authorisation criteria (as set out at paragraph 4.7 below) are met;*
- *what measures will be put in place to ensure proportionality is maintained (e.g. filtering, disregarding personal information);*
- *where an application is urgent, the supporting justification;*
- *any action which may be necessary to install, modify or remove software on the equipment;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results.”*

58. At §4.7-§4.9 of the EI Code the statutory tests for the issuing of a s. 5 warrant are highlighted, together with the statutory requirements for any urgent authorisation of a s. 5 warrant.

Renewals and cancellations of warrants

59. At §§4.10-4.11 and §§4.12-4.13 of the EI Code the provisions of the ISA addressing the renewals and cancellations of warrants are summarised.

Keeping of records

60. In Chapter 5 of the EI Code provision is made for centrally retrievable records of warrants to be kept for at least three years. At §5.1 it states:

“The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:

- *the date when a warrant is given;*
- *the details of what equipment interference has occurred;*
- *the result of periodic reviews of the warrants;*
- *the date of every renewal; and*
- *the date when any instruction was given by the Secretary of State to cease the equipment interference.”*

61. In the latest version of the EI Code, these requirements are expanded and §5.1 states:

“The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:

- ***all applications made for warrants and for renewals of warrants;***
- *the date when a warrant is given;*
- ***whether a warrant is approved under urgency procedures;***
- ***where any application is refused, the grounds for refusal as given by the Secretary of State;***
- *the details of what equipment interference has occurred;*
- *the result of periodic reviews of the warrants;*
- *the date of every renewal; and*
- *the date when any instruction was given by the Secretary of State to cease the equipment interference.”*

(items in bold are new requirements in this latest version of the Code)

Handling of information and safeguards

62. Chapter 6 of the EI Code provides important guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant and makes clear that this information may include communications content and communications data as defined in section 21 of RIPA (§6.1).

63. At §6.2 the EI Code states:

“The Intelligence Services must ensure that their actions when handling information obtained by means of equipment interference comply with the legal framework set out in the 1989 and 1994 Acts (including the arrangements in force under these Acts), the Data Protection Act 1998 and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with this legal

framework will ensure that the handling of information obtained by equipment interference continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards against abuse."

64. At §§6.6-6.11 of the EI Code key safeguards are set out in the EI Code in terms of the dissemination, copying, storage and destruction of any information obtained as a result of equipment interference. In particular it is stated:

"Dissemination of information

- 6.6 *The number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: information obtained by equipment interference must not be disclosed to any person unless that person's duties are such that he needs to know about the information to carry out those duties. In the same way only so much of the information may be disclosed as the recipient needs; for example if a summary of the information will suffice, no more than that should be disclosed.*
- 6.7 *The obligations apply not just to the Intelligence Service that obtained the information, but also to anyone to whom the information is subsequently disclosed. In some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further. In others, explicit safeguards may be applied to secondary recipients.*

Copying

- 6.8 *Information obtained by equipment interference may only be copied to the extent necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. Copies include not only direct copies of the whole of the information, but also extracts and summaries which identify themselves as the product of an equipment interference operation. The restrictions must be implemented by recording the making, distribution and destruction of any such copies, extracts and summaries that identify themselves as the product of an equipment interference operation.*

Storage

- 6.9 *Information obtained by equipment interference, and all copies, extracts and summaries of it, must [should] be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store such information securely applies to all those who are responsible for the handling of the information.*

Destruction

- 6.10 *Communications content, communications data and other information obtained by equipment interference, and all copies, extracts and summaries thereof, must [should] be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes set out in paragraph 6.5. If such*

information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid."

Personnel security

6.11 *In accordance with the need-to-know principle, each of the Intelligence Services must ensure [should] that information obtained by equipment interference is only disclosed to persons as necessary for the proper performance of the Intelligence Services' statutory functions. Persons viewing such product will usually require the relevant level of security clearance. Where it is necessary for an officer to disclose information outside the service, it is that officer's responsibility to ensure that the recipient has the necessary level of clearance."* (emphasis added)

65. At §§6.4-6.5 the importance of these safeguards is emphasised, together with the need to ensure that each of the Intelligence Services has **internal arrangements** in force for securing that the safeguards are satisfied, which arrangements should be made available to the Intelligence Services Commissioner. In particular it is stated:

"6.4 *Paragraphs 6.6 to 6.11 provide guidance as to the safeguards which must be applied by the Intelligence Services to the processing, retention, disclosure and destruction of all information obtained by equipment interference. Each of the Intelligence Services must ensure that there are internal arrangements in force, approved by the Secretary of State, for securing that these requirements are satisfied in relation to all information obtained by equipment interference.*

6.5 *These arrangements should be made available to the Intelligence Services Commissioner. The arrangements must ensure that the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act. Breaches of these handling arrangements must be reported to the Intelligence Services Commissioner as agreed with him."*

Application of the code to equipment interference pursuant to section 7 of the 1994 Act

66. In Chapter 7 of the EI Code it is made clear that "GCHQ must [should] as a matter of policy⁹ apply the provisions of this code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands" (§7.1).

67. Consequently, save as expressly specified in Chapter 7 of the EI Code, all of the provisions of the EI Code, including the important safeguards regarding the processing, retention, disclosure deletion and destruction of any information obtained via equipment interference, apply equally to equipment interference authorised pursuant to s. 7 of the ISA. That is made expressly clear in §7.2 which states:

"GCHQ and SIS must [should] apply all the same procedures and safeguards when conducting equipment interference authorised pursuant to section 7 as they do in relation to equipment interference authorised under section 5."

68. In addition, Chapter 7 of the EI Code provides specific additional guidance for s. 7 equipment

⁹ And without prejudice to arguments as to the applicability of the ECHR, as made clear in footnote 17 of the draft Code and footnote 18 of the November 2015 version.

interference authorisations under the ISA.

69. In terms of the general basis for lawful activity under s. 7 of the ISA, the EI Code states at §§7.3-7.6:

"7.3 *An authorisation under section 7 of the 1994 Act may be sought wherever members of SIS or GCHQ, or persons acting on their behalf or in their support, conduct equipment interference in relation to equipment located outside the British Islands that would otherwise be unlawful. This includes cases where the act is done in the British Islands, but is intended to be done in relation to apparatus that is or is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus.*

7.4 *If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a 'grace period' of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period).*

7.5 *An application for a section 7 authorisation should usually be made by a member of SIS or GCHQ for the taking of action in relation to that service. Responsibility for issuing authorisations under section 7 rests with the Secretary of State.*

7.6 *An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations. Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference must [should] be sought from a designated senior official (see paragraphs 7.11 to 7.14)."*

70. At §§7.7-7.8 and §§7.9-7.10 the EI Code sets out the statutory tests for s. 7 authorisations, together with the provisions of the statutory scheme dealing with urgent authorisations. At §7.7 the EI Code makes clear that:

"Each application should contain the same information, as far as is reasonably practicable in the circumstances, as an application for a section 5 equipment interference warrant."

71. Guidance on the types of authorisations under s.7 of the EI Code is also provided at §§7.11-7.14. In particular this provides guidance on any s. 7 authorisations which relate to a broad class of operations. At §§7.11-7.12 it states:

"7.11 *An authorisation under section 7 may relate to a broad class of operations. Authorisations of this nature are referred to specifically in section 7(4)(a) of the 1994 Act which provides that the Secretary of State may give an authorisation which inter alia relates to "acts of a description specified in the authorisation". The legal threshold for giving such an authorisation is the same as for a specific authorisation.*

7.12 *Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference must be sought from a designated senior official. In any case where the equipment interference may result in the acquisition of confidential information, authorisation must be sought from an Annex A approving officer. Where knowledge of matters subject to legal privilege may be acquired, the Annex A approving officer must apply the tests set out at paragraph 3.4 to 3.7 (and "Secretary of State" should be read as "Annex A approving officer" for these purposes).*

72. For GCHQ an 'Annex A approving officer' means a Director of GCHQ (see Annex A on page 30).

73. In addition §§7.13-7.14 provide guidance on all internal applications for approval, including the need to ensure that such approvals are proportionate and are subject to periodic review at least every 6 months, or more frequently depending on the sensitivity of the operation. Those paragraphs state:

"7.13 The application for approval must [should] set out the necessity, justification, proportionality and risks of the particular operation, and should contain the same information, as and where appropriate, as an application for a section 5 equipment interference warrant. Before granting the internal approval, the designated senior official or Annex A approving officer must [should] be satisfied that the operation is necessary for the proper discharge of the functions of the Intelligence Service, and that the taking of the action is proportionate to what the action seeks to achieve. The designated senior official or Annex A approving officer must consult the Foreign and Commonwealth Office or seek the endorsement of the Secretary of State for any particularly sensitive operations.

7.14 All internal approvals must [should] be subject to periodic review at least once every 6 months to ensure the operations continue to be necessary and proportionate. The approvals for particularly sensitive operations should be reviewed more frequently, depending on the merits of the case."

74. As to renewals and cancellations of s. 7 authorisations, the statutory requirements are set out at §§7.15-7.17.

Oversight by the Intelligence Services Commissioner

75. In §§8.1-8.2 of the EI Code the important role of the Intelligence Services Commissioner in the use of the powers under the ISA is emphasised. In particular §8.2 states:

"It is the duty of any member of the Intelligence Services who uses these powers to comply with any request made by the Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions. Such persons must also report any action that is believed to be contrary to the provisions of the 1994 Act to the Commissioner."

The Covert Surveillance and Property Interference Code ('the Property Code')

76. The Covert Surveillance and Property Interference Code ('the Property Code') provides guidance on entry on and interference with property by public authorities under s. 5 of the ISA (see the Code at §1.2).

77. Like the EI Code it was issued pursuant to s. 71 of RIPA. It was originally published in 2002 (called the 'Covert Surveillance Code of Practice') and a revised version was issued in 2010 (called the 'Covert Surveillance and Property Interference Revised Code of Practice'), with a further revised version published on 10 December 2014.
78. The Respondents have set out below the key provisions in the 2010/2014 version of the Code and in the 2002 version.
79. The changes as between the 2010 and the 2014 version of the Code are immaterial in terms of property interference activity by the Intelligence Services i.e. save for a few changes of paragraph number, the 2014 version did not alter the provisions relevant to these proceedings.

The 2010/2014 Property Code

80. Chapter 3 of the Code contains general rules on authorisations, *inter alia*, under s. 5 of the ISA. In particular guidance is given as to the requirement of proportionality. At §§3.3-3.7 the Code states:

“3.3 The ... 1994 Act stipulate[s] that the person granting an authorisation or warrant for ... interference with property, must believe that the activities to be authorised are necessary on one or more statutory grounds.

3.4 If the activities are deemed necessary on one of more of the statutory grounds, the person granting the authorisation or warrant must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

3.5 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3.6 The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;*
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.*

3.7 It is important therefore that all those involved in undertaking... interference with property under the ... 1994 Act are fully aware of the extent and limits of the authorisation or warrant in question.”

81. Consequently the Code draws specific attention to the need to balance the seriousness of the intrusion against the need for the activity in operational and investigative terms, including taking into account the effect on the privacy of any other person who may be affected i.e.

other than the subject of the operation. The Code is also very clear that it is important to consider all reasonable alternatives and to evidence what other methods were considered and why they were not implemented.

82. The question of collateral intrusion is also directly addressed in §§3.8ff of the Code. At §3.11 it states:

“Where it is proposed to conduct ... property interference specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy or property of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such ... property interference activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.3-3.8).”

83. As to the procedures to be followed for reviewing authorisations, the Code states at §§3.22-3.24 (these appear as §§3.23-3.25 in the 2014 version of the Property Code):

“3.22 Regular reviews of all authorisations should be undertaken to assess the need for the ... property interference activity to continue. The results of a review should be retained for at least three years (see Chapter 8). Particular attention is drawn to the need to review authorisations frequently where the ... property interference involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

3.23 In each case the frequency of reviews should be considered at the outset by the authorising officer or, for those subject to authorisation by the Secretary of State, the member or officer who made the application within the public authority concerned. This should be as frequently as is considered necessary and practicable.

3.24 In some cases it may be appropriate for an authorising officer to delegate the responsibility for conducting any reviews to a subordinate officer. The authorising officer is, however, usually best placed to assess whether the authorisation should continue or whether the criteria on which he based the original decision to grant an authorisation have changed sufficiently to cause the authorisation to be revoked. Support staff can do the necessary research and prepare the review process but the actual review is the responsibility of the original authorising officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

84. The Code highlights best working practices which are to be followed by all public authorities with regard to all activities covered by the Code at §§3.27ff (§3.28 in the 2014 version of the Property Code). At §3.28 it states:

3.28 Furthermore, it is considered good practice that within every relevant public authority, a senior responsible officer should be responsible for:

- the integrity of the process in place within the public authority to authorise ... property or wireless telegraphy;*
- compliance with ...this code;*
- engagement with the Commissioners and inspectors when they conduct their inspections, and where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.*

85. Chapter 4 of the Code contains special provisions on legally privileged and confidential information (see in particular §§4.10-4.15 and §§4.22-4.31).

86. Chapter 7 of the Code contains authorisation procedures for property interference. This specifically addresses authorisations for property interferences by the Intelligence Services. At §§7.36-7.38 it states:

"7.36 An application for a warrant must be made by a member of the intelligence services for the taking of action in relation to that agency. In addition, the Security Service may make an application for a warrant to act on behalf of the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ). SIS and GCHQ may not be granted a warrant for action in support of the prevention or detection of serious crime which relates to property in the British Islands.

7.37 The intelligence services should provide the same information as other agencies, as and where appropriate, when making applications for the grant or renewal of property warrants.

7.38 Before granting a warrant, the Secretary of State must:

- *think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;*
- *be satisfied that the taking of the action is proportionate to what the action seeks to achieve;*
- *take into account in deciding whether an authorisation is necessary and proportionate is whether the information which it is thought necessary to obtain by the conduct authorised by the warrant could reasonably be obtained by other means; and*
- *be satisfied that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of disclosure of any material obtained by means of the warrant, and that material obtained will be subject to those arrangements."*

The reference in §7.37 above to "the same information as other agencies" meant that, as and where appropriate §7.18 of the Code should be followed which provided:

7.18 Applications to the authorising officer for the granting or renewal of an authorisation must be made in writing (unless urgent) by a police officer, Revenue and Customs officer, SCDEA officer, a member of SOCA or an officer of the OFT and should specify:

- *the identity or identities, where known, of those who possess the property that is to be subject to the interference;*
- *sufficient information to identify the property which the entry or interference with will affect;*
- *the nature and extent of the proposed interference;*
- *the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;*
- *details of the offence suspected or committed;*
- *how the authorisation criteria (as set out above) have been met;*
- *any action which may be necessary to maintain any equipment, including replacing it;*
- *any action which may be necessary to retrieve any equipment;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and*
- *whether an authorisation was given or refused, by whom and the time and date on which this happened.*

87. In terms of renewals and cancellations of warrants by the Intelligence Services, §§7.39-7.42 of the Code state as follows:

"7.39 A warrant shall, unless renewed, cease to have effect at the end of the period of six

months beginning with the day on which it was issued (if the warrant was issued under the hand of the Secretary of State) or at the end of the period ending with the fifth working day following the day on which it was issued (in any other case).

7.40 If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of six months beginning with the day it would otherwise cease to have effect. ...

7.41 The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary.

7.42 The person who made the application to the Secretary of State must apply for its cancellation, if he is satisfied that the warrant no longer meets the criteria upon which it was authorised..."

88. Chapter 8 of the Code provides that certain records shall be kept of property interferences which are authorised. At §8.3 it states:

"8.3 The following information relating to all authorisations for property interference should be centrally retrievable for at least three years:

- the time and date when an authorisation is given;
- whether an authorisation is in written or oral form;

...

- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the authorisation;
- the date of every renewal; and
- the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy."

89. In Chapter 9 of the Code guidance is given as to the handling of material obtained through property interference. §9.3 of the Code addresses the retention and destruction of material and states as follows:

"9.3 Each public authority must ensure that arrangements are in place for the **secure handling, storage and destruction of material** obtained through the use of ... property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material." (emphasis added)

90. In addition the Code states at §9.7 that, in relation to the Intelligence Services:

"9.7 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the ... 1994 Act." (emphasis added)

91. Finally Chapter 10 of the Code highlights the oversight which is provided by the Intelligence Services Commissioner on the use of the powers under the ISA. At §10.2 it states:

"The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within ... the 1994 Act by ... GCHQ."

The 2002 Property Code

92. Chapter 2 of the Code contains general rules on authorisations, *inter alia*, under s. 5 of the ISA. Paragraph 2.10 specifically makes clear that the guidance on necessity and proportionality and on collateral intrusion in this part of the Code must be taken into account when applying for authorisations or warrants for entry onto or interference with property or with wireless telegraphy.
93. Consequently guidance is given as to the requirements of necessity and proportionality. At §§2.4-2.5 the Code states:
- "2.4 Obtaining an authorisation under the...1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.*
- 2.5 Then, if the activities are necessary; the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.*
94. The question of collateral intrusion is addressed in §§2.6-2.9 of the Code. In particular the following passages are relevant:
- 2.6 ...the authorising officer should take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.*
- 2.7 An application...should include an assessment of the risk of collateral intrusion. The authorising officer should take this into account, when considering the proportionality of the [property interference].*
95. In §2.19 of the Code it addresses obligations on the heads of the Intelligence Services and states:
- "The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services this is a statutory duty under the 1989 Act and the 1994 Act."*
96. In Chapter 3 of the Code provisions were set out addressing special rules on authorisations including on communications subject to legal privilege (§3.3ff) and communications involving confidential personal information and confidential journalistic material (§3.10ff).
97. Chapter 6 addressed the authorisation procedures for entry onto or interference with property under, *inter alia*, the ISA, including the duration of property warrants.
- 6.32 Before granting a warrant, the Secretary of State must:*
- *think it necessary for the action to be taken for the purpose of assisting the relevant agency in carrying out its functions;*

- *be satisfied that the taking of the action is proportionate to what the action seeks to achieve;*
- *take into account in deciding whether an authorisation is necessary and proportionate is whether the information which it is thought necessary to obtain by the conduct authorised by the warrant could reasonably be obtained by other means; and*
- *be satisfied that there are satisfactory arrangements in force under the 1994 Act or the 1989 Act in respect of disclosure of any material obtained by means of the warrant, and that material obtained will be subject to those arrangements."*

*6.34 A warrant shall, unless renewed, cease to have effect if the warrant was under the hand of the Secretary of State, at the end of the period of **six months** beginning with the day on which it was issued. In any other case, at the end of the period ending with the **second working day** following that day.*

*6.35 If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of **six months** beginning with that day. The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary."*

98. In addition §6.36 makes clear that:

6.26 The intelligence services should provide the same information as the police, as and where appropriate, when making applications, requests for renewal and requests for cancellation of property warrants.

99. Consequently the provisions at §6.9ff of the Code which set out the authorisation procedures for the police are also to be applied by the Intelligence Services as and where appropriate. These provisions include a detailed list of matters which should be included in any application for an authorisation – see §6.12 of the Code, including:

- *the identity or identities of those to be targeted (where known);*
- *the property which the entry or interference with will affect;*
- *the identity of the individuals and/or categories of people, where known, who are likely to be affected by collateral intrusion;*
- *details of the offence planned or committed;*
- *details of the intrusive surveillance involved;*
- *how the authorisation criteria...have been met;*
- *any action which may be necessary to retrieve any equipment used in the surveillance;*
- *in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and*
- *whether an authorisation was given or refused, by whom and the time and date."*

100. Finally Chapter 7 of the Code highlights the oversight which is provided by the Intelligence Services Commissioner on the use of the powers under the ISA. At §10.2 it states:

"The Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within ... the 1994 Act by ... GCHQ."

The HRA

101. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

*"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."*

102. Art. 10 of the ECHR, which is similarly a Convention right (and which is similarly set out in Sch. 1 to the HRA), provides:

*"(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*

103. By s. 6(1):

"It is unlawful for a public authority to act in a way which is incompatible with a Convention right."

104. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, GCHQ must (among other things) act proportionately and in accordance with law. In terms of equipment interference activity, the HRA applies at every stage of the process i.e. from authorisation, through to the obtaining, retention, handling and any disclosure/dissemination of such material.

105. S. 7(1) of the HRA provides in relevant part:

*"A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may—
(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ..."*

The DPA

106. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data (as defined in s. 1(1) of the DPA) that it holds. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.
107. Consequently as a data controller, GCHQ is in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other

things) the data protection principles if the exemption “is required for the purpose of safeguarding national security”. By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services (including GCHQ) are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services’ functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do not exempt the Intelligence Services (including GCHQ) from their obligation to comply with the fifth and seventh data protection principles, which provide:

“5. Personal data processed¹⁰ for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. ...

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”¹¹

108. Accordingly, when GCHQ obtains any information as a result of any property interference which amounts to personal data, it is obliged:
- (a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and
 - (b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

109. A member of the Intelligence Services commits an offence if “without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services”: s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member’s official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of GCHQ that is e.g. in breach of the relevant “arrangements” (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).
110. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

Oversight mechanisms

111. There are three principal oversight mechanisms in respect of the equipment interference regime:

¹⁰ The term “processing” is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

¹¹ The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

- (a) The Intelligence Services Commission
- (b) The ISC; and
- (c) The Tribunal.

The Intelligence Services Commissioner

112. As highlighted in the relevant Code, the Intelligence Services Commissioner's remit is to provide independent oversight of the use of the powers contained within the ISA by the Intelligence Services including GCHQ.
113. The Prime Minister is under a duty to appoint a Commissioner (see s. 59(1) of RIPA). By s. 59(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner is currently Sir Mark Waller.
114. Under s. 59(7) of RIPA, the Commissioner must be provided with such staff as are sufficient to ensure that he can properly carry out his functions. Those functions include those set out in s. 59(2), which provides in relevant part:
- "...the [Commissioner] shall keep under review, so far as they are not required to be kept under review by the Interception of Communications Commissioner-*
- (a) the exercise by the Secretary of State of his powers under sections 5 to 7 of... the Intelligence Services Act 1994..."*
115. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 60(1) of RIPA.
116. In practice, the Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Representative samples of warrantry paperwork are scrutinised, including the paperwork for s. 5 and/or s.7 ISA warrants/authorisations. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Commissioner also meets with the relevant Secretaries of State.
117. S. 60 of RIPA imposes important reporting duties on the Commissioner. (It is an indication of the importance attached to this aspect of the Commissioner's functions that reports are made to the Prime Minister.)
118. The Commissioner is by s. 60(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 60(3)). Pursuant to s. 60(4), a copy of each annual report (redacted, where necessary under s.60(5)), must be laid before each House of Parliament. In this way, the Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.
119. S. 58(5) grants the Commissioner power to make, at any time, any such other report to the Prime Minister on any other matter relating to the carrying out of his functions as he thinks fit.
120. In addition, the Commissioner is required by s. 59(3) to give the Tribunal:

“...such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-

- (a) in connection with the investigation of any matter by the Tribunal; or
- (b) otherwise for the purposes of the Tribunal’s consideration or determination of any matter.”

- 121. The Tribunal is also under a duty to ensure that the Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).
- 122. The Commissioner’s oversight functions are supported by the record keeping obligations that are imposed as part of the equipment interference regime, see §8.3 of the Code.
- 123. It is to be noted that in the *Liberty/Privacy* judgment the Tribunal placed considerable emphasis on the important oversight which is provided by the Interception Commissioner (see in particular §§24, 44, 91, 92 121 and 139 of the judgment) and a similarly important role is provided by the Intelligence Services Commissioner in the present context.

The ISC

- 124. GCHQ is responsible to the Foreign Secretary,¹² who in turn is responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.
- 125. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 (“the JSA”).
- 126. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.
- 127. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.
- 128. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the “ring of secrecy” which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.
- 129. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2)

¹² The Director of GCHQ must make an annual report on the work of GCHQ to the Prime Minister and the Secretary of State (see s. 4(4) of the ISA).

of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

130. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.

The Tribunal

131. The Tribunal was established by s. 65(1) of RIPA. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).
132. The Tribunal's jurisdiction is broad. As regards the Equipment Interference regime, the following aspects of the Tribunal's jurisdiction are of particular relevance:
- (a) The Tribunal has exclusive jurisdiction to consider claims under s. 7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).
 - (b) The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) of RIPA).
133. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).
134. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained, interfered with or disclosed information emanating from interferences with property/equipment in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged obtaining, interference with or disclosure of information.
135. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.¹³ As a result, the Tribunal is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.
136. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §134 above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) to provide it with assistance.

¹³ The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish e.g. that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

137. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.
138. Subject to any provision in its rules, the Tribunal may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

INTERNAL ARRANGEMENTS

139. GCHQ also has internal arrangements in relation to s.5 warrants and s.7 authorisations. These are set out below, with gisted passages underlined.

The Compliance Guide

140. The Compliance Guide is a document which is made available electronically to all GCHQ staff. The electronic version of the Compliance Guide was made available to staff in late 2008 and there have been no substantive changes since then, although it has been amended in minor ways to ensure that it remains up to date. It comprises mandatory policies and practices which apply to all GCHQ operational activity and has been approved by the Foreign Secretary and the Interception of Communications Commissioner. The Compliance Guide requires all GCHQ operational activity, including CNE activity, to be carried out in accordance with three core principles. These are that all operational activity must be:

- a) Authorised (generally through a warrant or equivalent legal authorisation);
- b) Necessary for one of GCHQ's operational purposes; and
- c) Proportionate.

141. These principles, and their application to specific activities conducted by GCHQ, are referred to throughout the Compliance Guide. They are also specifically referred to in the additional CNE-specific internal guidance referred to below. In short, they are core requirements which run through all the guidance which applies to GCHQ's operational activities, including CNE.

142. The section of the Compliance Guide which specifically concerns CNE states that authorisation is required under the ISA in order to address the liability which most CNE operations would normally attract under the Computer Misuse Act 1990. The requirement for a section 5 warrant for CNE operations on computers in the UK is made clear. Section 5 warrants are also addressed in the Compliance Guide as follows:

"A Secretary of State must approve a new ISA s.5 warrant. Renewal is required after six months. In an emergency, a new temporary warrant may be issued by a GCHQ official of appropriate seniority if a Secretary of State has expressly authorised its use."

Section 5 Guidance

143. GCHQ also has separate specific internal guidance governing applying for, renewing and cancelling section 5 warrants ("the Section 5 Guidance"). The Section 5 Guidance, application forms and warrant templates were updated following a visit of the Intelligence Services Commissioner (Sir Mark Waller) in June 2013. During that visit the Intelligence Services Commissioner acknowledged that GCHQ gave due consideration to privacy issues, but commented that he would like to see greater evidence of this reflected in warrants and submissions, in particular in relation to why the likely level of intrusion, both into the target's

privacy and the collateral intrusion into the privacy of others, was outweighed by the intelligence to be gained. In response, GCHQ updated its s.5 (as well as its s.7) application forms, warrant templates and guidance to advise staff on the type and level of detail required. At his next inspection in December 2013, the Intelligence Services Commissioner was provided with these documents and stated that he was content with the actions that had been taken.

144. The Section 5 Guidance makes clear the nature of the activity which is authorised by a s.5 warrant:

"ISA Section 5 guidance

ISA warrants

Warrants issued under the Intelligence Services Act (ISA) authorise interference with property (eg equipment such as computers, servers, routers, laptops, mobile phones, software, intellectual property etc) or wireless telegraphy."

145. The geographical, functional and temporal limits of a s.5 warrant are also set out:

"A section 5 warrant authorises interference with property or wireless telegraphy in the British Islands¹⁴...It may only be issued on grounds of National Security or the Economic Well-Being of the UK. A section 5 warrant is signed by a Secretary of State and is valid for 6 months from the date of signature, at which point the warrant should be renewed or cancelled."

146. The guidance mirrors the requirements of s.5(2)(a) and (b) of the ISA. First, it makes clear that the proposed CNE action must be **necessary**:

"Part I – to be completed by the relevant GCHQ team

The intelligence case should be fit for purpose for signing by a Secretary of State, avoiding unnecessary jargon and technical terminology. The case should include:

- *the intelligence background;*
- *the priority of the target within the priorities framework as endorsed by JIC¹⁵ and NSC¹⁶;*
- *an explanation of why the proposed operation is necessary;*
- *a description of any other agency involvement in working the target;*
- *the intelligence outcome(s) the proposed operation is expected to produce."*

147. The requirement that the proposed CNE action be **proportionate** is also made clear:

"As CNE techniques are by nature intrusive, an explanation of how proportionality will be maintained should be given. Key points to consider include:

- *the expected degree of invasion of a target's privacy and whether any personal or private information will be obtained;*
- *the likelihood of collateral intrusion, ie invading the privacy of those who are not targets of the operation, eg family members;*
- *whether the level of intrusion is proportionate to the expected intelligence benefit;*
- *a description of the measures to be taken to ensure proportionality."*

148. The Section 5 Guidance stipulates that each request for a warrant, or warrant renewal, must

¹⁴ Both instances of underlining in this quotation are in the original.

¹⁵ Joint Intelligence Committee.

¹⁶ National Security Council.

have a sponsor of an appropriately senior level:

"Requesting a new Section 5

Requests for new warrants and renewals must be sponsored by an appropriately senior official, who must be satisfied that the proposed operation is justified, proportionate and necessary."

149. The Section 5 Guidance requires that, once completed, the warrant request must be returned to its "sponsor" for consideration of whether it passes the test set out in s.5(2)(a) and (b) of the ISA, before being signed and sent to the relevant personnel:

"The form is then returned to the sponsor to consider whether, in light of the CNE input, they can recommend to the Secretary of State that the operation is justified, proportionate and necessary, and that they are aware of the risk. If so, they should sign and date the form and send it to the relevant personnel."

150. The Section 5 Guidance also explains that the process is completed by the preparation of a formal submission and a warrant instrument. These are reviewed by GCHQ Legal Advisers and the sponsor, then sent for signature to the relevant Department, which will follow its own internal procedures before the documents are passed to the Secretary of State for consideration. Once the warrant has been signed, relevant personnel will be informed that the operation can go ahead.

151. A designated form must be filled out when a section 5 warrant is sought. The specified information reflects the requirements of the guidance on section 5 warrants, and includes the following:

a) Under "Intelligence Case"

"why is CNE necessary and why can the expected intelligence not be gained by other less intrusive means¹⁷?"

"what intelligence the operation is expected to deliver

b) Under "Degree of intrusion, including collateral intrusion"

"how far will the operation intrude on the privacy of the target? Is the operation likely to obtain personal or private information?"

to what extent will the operation affect those not of operational interest (eg could the individual's computer be used by family members, friends or colleagues who are not targets of the operation)?

how will the intelligence gained justify the expected level of intrusion?

what measures will be put in place to ensure proportionality is maintained."

(c) Under "Recipients of Product":

"where within GCHQ is the product of the CNE operation to be sent?"

¹⁷ Underlining in the original.

(d) Finally, the Request must be authorised by the appropriately senior GCHQ official, who must, *inter alia*, certify that “*The proposed CNE operation is justified, proportionate and necessary*”.

Renewals of s.5 warrants

152. The Section 5 Guidance also details the procedure for renewals of section 5 warrants. This requires specific attention to be paid, *inter alia*, to whether the operation is still justified, necessary and proportionate at the time of the renewal:

Section 5 renewal process

A reasonable period before a warrant is due to expire, the relevant personnel will request a case for renewal from the relevant personnel, copying the sponsor and include a copy of the previous submission. The analyst should confirm with the sponsor that renewal is required, and if so, provide the relevant personnel with a business case by the specified deadline. This should include:

- *an update of the intelligence background, ensuring it accurately reflects the current context of the warrant;*
- *details of any developments and intelligence gained since the warrant was issued/last renewed – this **must** address any expectations highlighted in the previous submissions;*
- *a review of the level of intrusion, based on the evidence of the activity authorised by the warrant;*
- *a review and, if necessary, update of the political aspects of the risk assessment;*

The relevant team should provide the following information:

- *any updates on technical progress made since the warrant was last renewed*
- *an updated operational plan – again, this **must** address specific actions or plans laid out in the previous submission*
- *any updates to the risk assessment.*

Again, the relevant personnel may need to work with the originator and the relevant team to strengthen the renewal case, and will also consult the Legal Advisers before providing a copy to the sponsor for final review. When the sponsor is content that the submission is accurate and demonstrates that the operation is still justified, necessary and proportionate, the relevant personnel will submit the renewal application to the relevant Department for signature.”

Cancellation of s.5 warrants

153. The Section 5 Guidance also addresses cancellation of warrants, making clear that as soon as warrants are no longer required they should be cancelled:

“If a warrant is no longer required, it should be cancelled. If not renewed or cancelled, the warrant will expire on the date specified and the activity will no longer be authorised.

It is good practice to cancel warrants as soon as the requirement for the operation has ceased.

Section 5 cancellation process

When a warrant is no longer required, the analyst should send the relevant personnel a short explanation of the reason for the cancellation. When the team conducting the operation confirms that the operation is fully drawn down, the relevant personnel will draft a letter based on this feedback and submit it, with a cancellation instrument, to the issuing Department for signature (usually by a senior official rather than the Secretary of State).”

Section 7 Guidance

154. GCHQ's guidance which governs applying for, renewing and cancelling section 7 authorisations/internal approvals is set out both in the Compliance Guide (in the section dealing with authorisations) and in separate internal guidance ("the Section 7 Guidance"). The process set out in the Section 7 Guidance has been subject to the scrutiny and advice of the Intelligence Services Commissioner who has confirmed that he is content with the process.¹⁸
155. The Section 7 Guidance requires any CNE activities overseas to be carried out pursuant to a s.7 authorisation in order for such activities to be lawful under domestic law. Authorisations may either be specific to a particular operation or to a broad class of operation:

"ISA Section 7 guidance

ISA authorisations

An ISA s7 authorisation given by the Secretary of State is the legal instrument that removes criminal liability in the UK for GCHQ actions overseas which might otherwise be an offence in UK law. Such an authorisation is also capable of removing any civil liability in the UK that might arise as a result of GCHQ's actions overseas. GCHQ primarily uses s7 authorisations for CNE operations. An ISA s7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations..."

156. The Section 7 Guidance sets out the 'class authorisations' signed by the Secretary of State under section 7 of the ISA which are used by GCHQ for the majority of its active internet-related operations. In respect of the authorisations relevant to CNE the Section 7 Guidance states that it:

"permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant). The interference includes CNE operations."

157. The Section 7 Guidance also stipulates that such authorisations need to be renewed every six months, and assert the vital importance of providing information to the Secretary of State to justify any renewal:

"Class authorisations are signed by the Foreign Secretary and need to be renewed every six months. Relevant personnel in GCHQ are responsible for overseeing the renewal process. Prior to expiry of the authorisations, they will ask analysts to briefly (re)justify the necessity and proportionality of continuing to rely on all extent section 7 internal approvals for which they are the lead, as well as asking for feedback on the outcomes of operations conducted. Providing feedback to the Foreign Secretary on the value of operations conducted under the class authorisations is crucial in justifying their renewal."

158. The requirement, in addition to a section 7 class authorisation, for a section 7 approval for a

¹⁸ In addition to the Intelligence Services Commissioner's suggestions in his June 2013 inspection, and his approval of GCHQ's consequent changes in his December 2013 inspection, during a visit in December 2014 GCHQ presented to and discussed with the Intelligence Services Commissioner, the "end to end" process regarding CNE operations using two operational case-studies. The class-authorisation, internal approvals and additions authorisations were considered. The Commissioner was then shown how CNE operators conduct the operations with a live demonstration of an operation. There was also a focus on the relevant forms (which were discussed in some detail). The Commissioner indicated that he was content with the format and the level of detail in the forms.

specific operation, and the procedure for obtaining such an approval, is set out both in the section of the Compliance Guide on CNE, and also in the Section 7 Guidance. The latter emphasises, *inter alia*, the importance of considering and setting out, in a request for a section 7 approval, why an operation against a target is necessary and proportionate, and the requirement that a copy of the signed approval be sent to the FCO:

“ISA section 7 internal approvals

A condition of section 7 authorisations is that GCHQ operates an internal section 7 approval process to record its reliance on these authorisations. Before tasking the operational team to conduct CNE operations, analysts are required to complete a request form including a detailed business case described the necessity and proportionality of conducting operations against the targets. The request also sets out the likely political risk. The request must be endorsed by a senior member of the operational team before it is passed to an appropriately senior official for approval...A copy of the signed final version of the approval is sent to FCO for information.”

159. The Section 7 Guidance explains the importance of this process, including the provision of signed approvals to the FCO, for ensuring that operations are necessary, justified and proportionate is again stressed:

“This process provides the necessary reassurance to FCO that operations carried out under the class authorisations are necessary, justified and proportionate.”

160. Necessity (including why means other than a CNE operation could not be used) and proportionality (particularly with regard to the privacy of a target or any third party) are addressed in more detail under “Section B – business case/necessity/proportionality”:

“The business case should...include:

- the intelligence background;*
- the priority in the priorities framework;*
- an explanation of why the operations against the target set are necessary;*
- the intelligence outcome(s) the proposed CNE activities are expected to produce.”*

You should also consider the level of intrusion the proposed operations will involve and how proportionality will be maintained. Key points to consider include:

- the expected degree of intrusion into a target’s privacy and whether any personal or private information will be obtained;*
- the likelihood of collateral intrusion, i.e. invading the privacy of those who are not targets, such as family members;*
- whether the level of intrusion is proportionate to the expected intelligence benefit;*
- any measures to be taken to ensure proportionality.”*

161. The Section 7 Guidance makes clear, under “Completing the process” that the internal approval will then be provided to an appropriately senior GCHQ official for signature and for, *inter alia*, the setting of a review period for the internal approval:

“Based on all the information provided, relevant personnel will ensure that the section 7 internal approval is suitable for referral to an appropriately senior GCHQ official for signature. That official will review all the matters relevant to the application to satisfy himself that the proposed activity is justified, necessary and proportionate, including validating the assessment of political risk. He will also set the review period for the internal approval, which will be shorter for particularly sensitive operations.”

162. The standard form used for seeking section 7 approvals reflects both the Section 7 Guidance

and the statutory criteria. In particular it sets out the following:

- a) **"Business case, including"**
 - *Intelligence background (to include brief details of what has been achieved from other accesses).*
 - *What you expect to get from using CNE techniques against this target set & how the intelligence gained will justify the expected level of intrusion.*
 - *Any timing factors or special sensitivities.*
- b) **"Necessity, including"**
 - *The necessity of conducting CNE operations against this target set (an explanation of why the use of CNE techniques is necessary)."*
- c) **"Proportionality and consideration of intrusion into privacy, including"**
 - *The proportionality of conducting CNE operations against this target set (CNE operations are intrusive by nature, and are likely to obtain information which is personal and private). Confirm that you have assessed that the level of intrusion into privacy, including collateral intrusion, is justified and proportionate. Outline measures to be put in place to ensure proportionality is maintained."*

The term "privacy" is defined "in the broadest sense to mean a state in which one is not observed or disturbed by others".

163. The appropriately senior GCHQ official who must support any request for a section 7 approval has to certify, *inter alia*, that:

"Operations conducted under this approval are justified, proportionate and necessary."
164. The relevant form also makes clear that the request for an approval should be sent to the relevant personnel at request stage, review stage and cancellation stage. Where an addition to an approval is sought the relevant personnel must also be consulted.¹⁹ As a matter of practice, and as required by the Section 7 Guidance, final versions of s.7 approvals are sent to the Foreign and Commonwealth Office. A monthly summary report which summarises new s.7 approvals, reviews of s.7 approvals and cancellations, and also attaches copies of new approvals, is also sent to the relevant senior official at the FCO.
165. The Section 7 Guidance also deals with the situation where there is a significant change to an existing approval, or when a new target is proposed with the result that an "addition" to an existing approval is required.
166. The "additions form" requires the same regard to be had to justification, necessity and proportionality as is required for an initial approval.

Review of s.7 internal approvals

167. Approvals must be reviewed, and upon each review consideration is required to be given to whether the operation is still necessary and proportionate, specifically having regard to issues of intrusion and privacy. The process of reviewing s.7 approvals is summarised in the Section 7 Guidance as follows:

¹⁹ A reference to "relevant personnel" is to staff who are responsible for securing legal/policy approvals, checking the relevant risk assessments and maintaining compliance records.

"Reviewing section 7 internal approvals

In addition to the reviews that are carried out in support of the renewal of the class authorisations when analysts are required to briefly (re)justify the necessity and proportionality of continuing to rely on all extant internal approvals for which they are the lead, there is a rolling programme of fully revalidating all extant section 7 internal approvals. This revalidation mirrors the process for obtaining a new internal approval: an updated business case (covering justification, necessity, proportionality and intrusion into privacy) is provided by the lead analyst; the operational team confirm that they are still operating within the risk thresholds set when the internal approval was signed; the endorser confirms that the assessment of the likely political risk is still correct; then continued operations may be approved and a new review date set if no significant changes have been made (or the review of the approval is passed to a GCHQ official of appropriate seniority."

168. The review and revalidation is held at intervals determined by the designated GCHQ senior official who originally signed the section 7 approval. These are more frequent for particularly sensitive operations. The Section 7 Guidance also sets out a procedure for recording the history of a section 7 approval from the original submission through to any review or cancellation:

"New review history and cancellation forms will be appended at each review point. The intention is to leave the original submission intact, so that there is an audit trail of what was originally submitted/approved. If there are any updates to be made, these will be included in the review history so that there is an ongoing record at each review of what was decided and why."

169. Thus the approval process, including any review, is recorded so that the history of and basis (including necessity and proportionality) for any approval, review or cancellation, is available for audit.

Cancellation of s. 7 internal approvals

170. The Section 7 Guidance also stipulates the need to cancel internal approvals as soon as an operation is no longer needed:

"Cancelling a section 7 internal approval

To show due diligence and as a condition of relying on the class authorisations, section 7 internal approvals should be cancelled when an operation is no longer needed. To help ensure that this happens, the relevant personnel will ask whether section 7 internal approvals are still needed as part of the class authorisation renewals process, and if so will seek a brief rejustification of the continuing necessity and proportionality. The number of approvals signed or cancelled is provided to the Foreign Secretary with the case for renewal.

It is important to cancel an internal approval as soon as it is no longer required.

When a section 7 internal approval is no longer required, the analyst should ask the operational team point of contact to cease operations and remove all tasking. The relevant personnel will not formally cancel the approval until the operational team confirms that the operation is fully drawn down."

171. The Section 7 Guidance therefore contains safeguards against section 7 approvals remaining in place where they are no longer necessary and/or proportionate.

Obtaining data

172. There are further safeguards in place to ensure that decisions by CNE operators to obtain data from implanted devices are lawful. In particular:
- a) In addition to a formal process of training and examination which all CNE Operators have to undergo, all CNE operators must every two years also undertake advanced legalities training which is specific to active operations such as CNE (in addition to the basic legalities training which all staff are required to complete).
 - b) CNE operators can obtain legal advice at any time.
 - c) In addition, any data obtained in an operation will be available to the relevant intelligence analysts for that project, who in turn will be aware of the legal authorisation for the project, and will also have completed legalities training. The CNE section of the Compliance Guide provides guidance for intelligence for intelligence analysts requesting a particular document to be retrieved.
173. Thus, the obtaining of data is subject to the same requirements of necessity and proportionality as the initial process of obtaining an authorisation/warrant/approval.

Storage of and access to data

174. GCHQ also has policies for storage of and access to data obtained by CNE.
175. The section of the Compliance Guide concerning "Review and Retention" states that GCHQ treats "all operational data" (i.e. including that obtained by CNE) as if it were obtained under RIPA. It sets out GCHQ's arrangements for minimising retention of data in accordance with RIPA safeguards. This is achieved by setting default maximum limits for storage of operational data.
176. In addition GCHQ has a separate policy specifically concerning data storage and access. It defines different categories of data, and importantly ascribes specific periods for which different categories of data may be kept, as well as explaining how different categories of CNE data relate to the categories of operational data set out in the Compliance Guide.
177. Where CNE analysts identify material as being of use for longer periods than the stipulated limits, it can be retained for longer, subject to justification according to specific criteria.
178. Access to data is also subject to strict safeguards, which are set out in the Compliance Guide. CNE content may be accessed by intelligence analysts, but they must first demonstrate that such access is necessary and proportionate by completing a Human Rights Act ("HRA") justification. HRA justifications are recorded and made available for audit. CNE technical data relating to the conduct of CNE operations may only be accessed by a team of trained operators responsible for planning and running such operations.
179. GCHQ's policy on storage of and access to data also requires GCHQ analysts who are not in the CNE operational unit to justify access to CNE data on ECHR grounds (particularly necessity and proportionality). The justification must be recorded and available for audit.

Handling/disclosure/sharing of data obtained by CNE operations

180. Pursuant to GCHQ's Compliance Guide, the position is that all operational material is handled, disclosed and shared as though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

181. The general rules, as set out in the Compliance Guide and the Intelligence Sharing and Release Policy which apply to the handling of operational material include, *inter alia*, a requirement for mandatory training on operational legalities and detailed rules on the disclosure of such material outside GCHQ and the need to ensure that all reports are disseminated only to those who need to see them.

a) Operational data cannot be disclosed outside of GCHQ other than in the form of an intelligence report.

b) Insofar as operational data comprises or contains confidential information (e.g. journalistic material) then any analysis or reporting of such data must comply with the "Communications Containing Confidential Information" section of the Compliance Guide. This requires GCHQ to have greater regard to privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved (e.g. legally privileged material, confidential personal information, confidential journalistic information, communications with UK legislators). GCHQ must accordingly demonstrate to a higher level than normal that retention and dissemination of such information is necessary and proportionate.

Training

182. In addition to the training referred to at paragraphs 172(a) and 181 above, GCHQ does provide some training for analysts on particular CNE activities, which reiterates the substance of the Section 7 Guidance. GCHQ is currently in the process of revising the training referred to at paragraph (172(c)) to incorporate more detail on CNE.

0

0



Neutral Citation Number: [2016] UKIP Trib 14_85-CH
IN THE INVESTIGATORY POWERS TRIBUNAL

P.O. Box 33220
London
SW1H 9ZQ
Date: 12/02/2016

Before :

MR JUSTICE BURTON (PRESIDENT)
MR JUSTICE MITTING (VICE-PRESIDENT)
MR ROBERT SEABROOK QC
MR CHARLES FLINT QC
THE HON CHRISTOPHER GARDNER QC

Between :

Case No.
IPT 14/85/CH

PRIVACY INTERNATIONAL
- and -

Claimant

(1) THE SECRETARY OF STATE FOR
FOREIGN AND COMMONWEALTH AFFAIRS
(2) THE GOVERNMENT COMMUNICATIONS
HEADQUARTERS

Respondents

Case No. IPT
14/120-126/CH

GREENNET LIMITED
RISEUP NETWORKS, INC
MANGO EMAIL SERVICE
KOREAN PROGRESSIVE NETWORK
("JINBONET")
GREENHOST
MEDIA JUMPSTART, INC
CHAOS COMPUTER CLUB
- and -

Claimants

(1) THE SECRETARY OF STATE FOR
FOREIGN AND COMMONWEALTH AFFAIRS
(2) THE GOVERNMENT COMMUNICATIONS
HEADQUARTERS

Respondents

Ben Jaffey and Tom Cleaver (instructed by Bhatt Murphy Solicitors) for the
Claimants

James Eadie QC, Daniel Beard QC, Kate Grange and Richard O'Brien (instructed
by Government Legal Department) for the Respondents

Jonathan Glasson QC, Counsel to the Tribunal (instructed by Government Legal
Department)

Hearing dates: 1, 2 and 3 December 2015

Approved judgment

Mr Justice Burton (The President):

1. This is the judgment of the Tribunal.
2. This has been a hearing in respect of the claim by Privacy International, the well known NGO, and seven internet service providers, of which Greenet Limited carries on operations in this country and the other Claimants have customers in this country, though their main operations are based abroad. The hearing has been of preliminary issues of law, whose purpose is to establish whether, if the Second Respondent ("GCHQ") carries on the activity which is described as CNE (Computer Network Exploitation), which may have affected the Claimants, it has been lawful. The now well established procedure for this Tribunal is to make assumptions as to the significant facts in favour of claimants and reach conclusions on that basis, and only once it is concluded whether or not, if the assumed facts were established, the respondent's conduct would be unlawful, to consider the position thereafter in closed session. This procedure has enabled the Tribunal, on what is now a number of occasions, to hold open inter partes hearings, without possible damage to national security, while preserving, where appropriate, the Respondents' proper position of Neither Confirmed Nor Denied ("NCND").
3. Various possible different methods or consequences of CNE, or in its colloquial form 'hacking', as summarised in paragraph 9 below, have been canvassed in the witness statements produced on behalf of the Claimants by Mr Eric King, Professor Ross Anderson and Professor Peter Sommer, to which there have been responses, always subject to the constraints of NCND, in the witness statements of Mr Ciaran Martin, the Director General of Cyber Security at GCHQ. The particular significance of the use of CNE is that it addresses difficulties for the Intelligence Agencies caused by the ever increasing use of encryption by those whom the Agencies would wish to target for interception. The Claimants point out that CNE inevitably goes beyond interception, in accessing what is not and would not be communicated. The context of the issue is that the security situation for the United Kingdom, presently described as severe, is such that there needs to be the most diligent possible protection by the Respondents of the citizens and residents of the UK. Mr Martin points out in his first witness statement that even in the past year the threat to the UK from international terrorism in particular has continued to increase, and Mr Eadie QC for the Respondents submitted that proper protection of the citizen against terrorist attack is of the most fundamental importance, and that technological capabilities operated by the Intelligence Agencies lie at the very heart of the attempts of the State to safeguard the citizen against terrorist attack.
4. The sections of the Intelligence Services Act 1994 ("ISA") which have been primarily under consideration at this hearing are s.3, which sets out the powers of GCHQ, s.5 (with its machinery in part set out in s.6) and s.7. We shall refer to a s.5 warrant and a s.7 authorisation:

*"3. The Government Communications
Headquarters.*

(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be -

- (a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and*
- (b) to provide advice and assistance about—*
 - (i) languages, including terminology used for technical matters, and*
 - (ii) cryptography and other matters relating to the protection of information and other material,*

to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

(2) The functions referred to in subsection (1)(a) above shall be exercisable only—

- (a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or*
- (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or*
- (c) in support of the prevention or detection of serious crime.*

5 Warrants: general.

(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is

authorised by a warrant issued by the Secretary of State under this section.

(2) The Secretary of State may, on an application made by . . . GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State -

- (a) thinks it necessary for the action to be taken for the purpose of assisting . . .*
- (iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and*
- (b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;*
- (c) is satisfied that satisfactory arrangements are in force under section 2(2)(a) of the [Security Service Act 1989 ("the 1989 Act")] (duties of the Director-General of the Security Service), section 2(2)(a) above or section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements.*

(2A) The matters to be taken into account in considering whether the requirements of subsection (2)(a) and (b) are satisfied in the case of any warrant shall include whether what it is thought necessary to achieve by the conduct authorised by the warrant could reasonably be achieved by other means.

(3) A warrant issued on the application of the Intelligence Service or GCHQ for the purposes of the exercise of their functions by virtue of section . . . 3(2)(c) above may not relate to property in the British Islands.

(3A) A warrant issued on the application of the Security Service for the purposes of the exercise of their function under section 1(4) of the Security

Service Act 1989 may not relate to property in the British Islands unless it authorises the taking of action in relation to conduct within subsection (3B) below.

(3B) Conduct is within this subsection if it constitutes (or, if it took place in the United Kingdom, would constitute) one or more offences, and either -

- (a) it involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose; or*
- (b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more.*

(4) Subject to subsection (5) below, the Security Service may make an application under subsection (2) above for a warrant to be issued authorising that Service (or a person acting on its behalf) to take such action as is specified in the warrant on behalf of the Intelligence Service or GCHQ and, where such a warrant is issued, the functions of the Security Service shall include the carrying out of the action so specified, whether or not it would otherwise be within its functions.

(5) The Security Service may not make an application for a warrant by virtue of subsection (4) above except where the action proposed to be authorised by the warrant—

- (a) is action in respect of which the Intelligence Service or, as the case may be, GCHQ could make such an application; and*
- (b) is to be taken otherwise than in support of the prevention or detection of serious crime*

6 Warrants: procedure and duration, etc.

(1) A warrant shall not be issued except—

- (a) *under the hand of the Secretary of State or in the case of a warrant by the Scottish Minister (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive; or*
 - (b) *in an urgent case where the Secretary of State has expressly authorised its issue and a statement of that fact is endorsed on it, under the hand of a senior official; or*
 - (c) *in an urgent case where, the Scottish Ministers have (by virtue of provision made under section 63 of the Scotland Act 1998) expressly authorised its issue and a statement of that fact is endorsed thereon, under the hand of a member of the staff of the Scottish Administration who is in the Senior Civil Service and is designated by the Scottish Ministers as a person under whose hand a warrant may be issued in such a case.*
 - (d) *in an urgent case where the Secretary of State has expressly authorised the issue of warrants in accordance with this paragraph by specified senior officials and a statement of that fact is endorsed on the warrant, under the hand of the specified officials.*
- (1A) *But a warrant issued in accordance with subsection (1) (d) may authorise the taking of an action only if the action is an action in relation to property which, immediately before the issue of the warrant, would, if done outside the British Islands, have been authorised by virtue of an authorisation under section 7 that was in force at that time.*
- (1B) *A senior official who issues a warrant in accordance with subsection (1)(d) must inform the Secretary of State about the issue of the warrant as soon as practicable after issuing it."*
- (2) *A warrant shall, unless renewed under subsection (3) below, cease to have effect—*
- (a) *if the warrant was under the hand of the Secretary of State or, in the case of a*

warrant issued by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive, at the end of the period of six months beginning with the day on which it was issued; and

(b) in any other case, at the end of the period ending with the second working day following that day.

(3) If at any time before the day on which a warrant would cease to have effect the Secretary of State considers it necessary for the warrant to continue to have effect for the purpose for which it was issued, he may by an instrument under his hand renew it for a period of six months beginning with that day.

(4) The Secretary of State shall cancel a warrant if he is satisfied that the action authorised by it is no longer necessary.

(5) In the preceding provisions of this section "warrant" means a warrant under section 5 above.

...

7 Authorisation of acts outside the British Islands.

(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.

(2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom.

(3) The Secretary of State shall not give an authorisation under this section unless he is satisfied -

(a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a

function of the Intelligence Service or GCHQ; and

(b) that there are satisfactory arrangements in force to secure -

(i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of the Intelligence Service or GCHQ; and

(ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and

(c) that there are satisfactory arrangements in force under section 2(2)(a) or 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.

(4) Without prejudice to the generality of the power of the Secretary of State to give an authorisation under this section, such an authorisation -

(a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;

(b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified.

(5) An authorisation shall not be given under this section except -

(a) under the hand of the Secretary of State; or

(b) in an urgent case where the Secretary of State has expressly authorised it to be

given and a statement of that fact is endorsed on it, under the hand of a senior official.

(6) An authorisation shall, unless renewed under subsection (7) below, cease to have effect -

- (a) if the authorisation was given under the hand of the Secretary of State, at the end of the period of six months beginning with the day on which it was given;*
- (b) in any other case, at the end of the period ending with the second working day following the day on which it was given.*

(7) If at any time before the day on which an authorisation would cease to have effect the Secretary of State considers it necessary for the authorisation to continue to have effect for the purpose for which it was given, he may by an instrument under his hand renew it for a period of six months beginning with that day.

(8) The Secretary of State shall cancel an authorisation if he is satisfied that any act authorised by it is no longer necessary.

(9) For the purposes of this section the reference in subsection (1) to an act done outside the British Islands includes a reference to any act which -

- (a) is done in the British Islands; but*
- (b) is or is intended to be done in relation to apparatus that is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus;*

and in this subsection "apparatus" has the same meaning as in [RIPA].

(10) Where-

- (a) a person is authorised by virtue of this section to do an act outside the British Islands in relation to property,*
- (b) the act is one which, in relation to property within the British Islands, is*

capable of being authorised by a warrant under section 5,

- (c) a person authorised by virtue of this section to do that act outside the British Islands, does the act in relation to that property while it is within the British Islands, and*
- (d) the act is done in circumstances falling within subsection (11) or (12),*

This section shall have effect as if the act were done outside the British Islands in relation to that property.

(11) An act is done in circumstances falling within this subsection if it is done in relation to the property at a time when it is believed to be outside the British Islands.

(12) An act is done in circumstances falling within this subsection if it—

- (a) is done in relation to property which was mistakenly believed to be outside the British Islands either when the authorisation under this section was given or at a subsequent time or which has been brought within the British Islands since the giving of the authorisation; but*
- (b) is done before the end of the fifth working day after the day on which the presence of the property in the British Islands first becomes known.*

(13) In subsection (12) the reference to the day on which the presence of the property in the British Islands first becomes known is a reference to the day on which it first appears to a member of the Intelligence Service or of GCHQ, after the relevant time—

- (a) that the belief that the property was outside the British Islands was mistaken; or*
- (b) that the property is within those Islands.*

(14) In subsection (13) 'the relevant time' means, as the case may be –

- (a) the time of the mistaken belief mentioned in subsection (12)(a); or
- (b) the time at which the property was, or was most recently, brought within the British Islands."

5. The 'assumed facts' procedure has been impacted to an extent on this occasion by virtue of the fact that there has been a considerable degree of acceptance by the Respondents, or 'avowal' as it has been called, of the existence and use of CNE by GCHQ, and certainly so since the publication on 6 February 2015, during the course of, and seemingly as a direct result of, the existence of these proceedings, of the draft Equipment Interference Code of Practice pursuant to s.71 of the Regulation of Investigatory Powers Act 2000 ("RIPA") ("the E I Code"), which has now, after a period of consultation, been laid before Parliament in November 2015. [Since the hearing, it has been brought into force by S.I.2016 no.38 dated 14 January 2016]. As a result of a Schedule of Avowals, helpfully prepared by Mr Jaffey of counsel on behalf of the Claimants, and responded to by the Respondents, the following matters are admitted:
- i) GCHQ carries out CNE within and outside the UK.
 - ii) In 2013 about 20% of GCHQ's intelligence reports contained information derived from CNE.
 - iii) GCHQ undertakes both "*persistent*" and "*non-persistent*" CNE operations, namely both where an 'implant' expires at the end of a user's internet session and where it "*resides*" on a computer for an extended period.
 - iv) CNE operations undertaken by GCHQ can be against a specific device or a computer network.
 - v) GCHQ has obtained warrants under s.5 and authorisations under s.7, and in relation to the latter had five s.7 class based authorisations in 2014.
6. Apart from the provisions of the ISA, the other most material statutory provisions are as follows:
- i) The 1989 Act (referred to above) by s.3 gave the power to the Security Service ("MI5") to apply for a warrant, which it is common ground could have authorised conduct by GCHQ (whose existence was not at that stage publicly admitted) on its behalf, whereby the Secretary of State could, on an application made by MI5 issue a warrant "*authorising the taking of such action as is specified in the warrant in*

respect of any property so specified in the circumstances there provided for. This provision was replaced by ISA in 1994.

- ii) The Official Secrets Act 1989 makes it an offence for a member of the Security and Intelligence Services by s.1 to disclose information relating to security or intelligence without lawful authority and by s.8 to retain it without lawful authority or fail to take proper care to prevent unauthorised disclosure of it.
- iii) A similar provision to safeguard information obtained by any of the Intelligence Services, by limiting its disclosure and use to the proper discharge of any of their functions (including the interests of national security) is in s.19 of the Counter-Terrorism Act 2008.
- iv) The provisions of the Data Protection Act 1998 preserve (notwithstanding any exemptions) the obligation on GCHQ to comply with the Fifth and Seventh data protection principles, namely:

"5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. ...

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

- 7. The Respondents accept and assert that as a matter of public law they have been bound since February 2015 by the draft E I Code, which was accompanied by a Ministerial statement to that effect. We are satisfied that that is the case. Prior to such publication, there was the Covert Surveillance and Property Interference Code (the "Property Code"), also pursuant to s.71 of RIPA, which has been materially in its present form since 2002. The Property Code continues in force, but under paragraph 1.2 of the E I Code where there is an overlap between the two Codes the E I Code takes precedence.
- 8. The parties agreed a List of Issues to be resolved at the hearing, which were agreed during the period of preparation for the hearing as a result of excellent cooperation between the parties, and with the very considerable assistance of Jonathan Glasson QC, Counsel for the Tribunal. As a result of the very careful preparation for, and the concise and persuasive presentation at, the hearing by both parties, it was possible to conclude the oral argument in 3 days. There was a degree of context for the resolution of the issues, not just by reference to the witness statements to which we have referred. The Respondents accept that the provisions of Articles 8 and 10 of the European Convention of Human Rights, which we do not need to set out, apply to Privacy International as a campaigning NGO, and, at least for the purposes of this hearing, that they both apply to the internet companies: in any event there is no material difference in the applicability of both Articles, which have been, as in previous hearings, argued in tandem. As to other matters:

- i) Both parties accepted at this hearing the effect of this Tribunal's conclusions in what have become known as Liberty/Privacy (No.1) [2015] 3 AER 142 and (No.2) [2015] 3 AER 212. It was common ground that all the material decisions of the ECtHR were fully canvassed in Liberty/Privacy (No.1) and their effect set out in that Judgment. The consequence was that there was a great deal less need to refer to the underlying ECtHR Judgments themselves in the hearing before us, and it was common ground that the only material ECtHR decision since Liberty/Privacy is R.E. v United Kingdom (Application No.62498/11), Judgment 27 October 2015, to which we were referred by both sides.
 - ii) As in Liberty/Privacy, emphasis was placed by the Respondents on the existence of oversight of the security arrangements and procedures by the Intelligence and Security Committee of Parliament ("ISC") and by the Commissioners. In this case the relevant Commissioner is the Intelligence Services Commissioner, Sir Mark Waller, on whose Reports both sides relied. As is to be expected, and will be referred to below, Sir Mark's responsibility included drawing attention to areas which, upon his inspection of the Intelligence Services, he felt could be improved; but there is no doubt, by reference to those Reports, that it continues to be his view, as expressed in his 2013 Report, that "*GCHQ's staff continue to conduct themselves with the highest level of integrity and legal compliance*". The ISC's latest report of 12 March 2015 is to similar effect.
9. It was agreed for the purpose of the List of Issues (at paragraph 6) that CNE might be used by GCHQ so as to involve the following:
- a) The obtaining of information from a particular device, server or network.

That constituted part of the Respondents' avowals, and consequently was no longer subject to NCND. As to the balance of the original paragraph 6 of the List of Issues:

- b) The creation, modification or deletion of information on a device, server or network.

It was accepted at paragraph 46 of Mr Martin's First Statement that CNE could theoretically change the material on a computer, e.g. by way of an implant. In the light of that, coupled with the acceptance generally by GCHQ that it carries out CNE activities, GCHQ accepts that it has avowed the creation (to the extent that the placing of an implant on a device amounts to the creation of information) and modification of information on a device and this is no longer subject to NCND. In addition, whilst GCHQ accepts that creating or modifying information on a server or network could lawfully occur, this is neither confirmed nor denied.

But apart from that, sub-paragraph (b) is neither confirmed nor denied.

- c) The carrying out of intrusive surveillance.

This is neither confirmed nor denied, although GCHQ has accepted that the use of CNE techniques may be intrusive.

- d) The use of CNE in such a way that it creates a potential security vulnerability in software or hardware, on a server or on a network.

This is not avowed. However it has been accepted that any CNE operations which are carried out by GCHQ are conducted in such a way as to minimise the risk of leaving target devices open to exploitation by others (see paragraph 39 of Mr Martin's First Statement).

- e) The use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest.

This has been characterised as 'bulk CNE'. The Respondents agree that this could arise pursuant to the powers of GCHQ within the scope of a s.7 authorisation, but neither admit nor deny that it has ever occurred, and Mr Martin in his third witness statement says that it is "*simply not correct to assert that GCHQ is using CNE on an indiscriminate and disproportionate scale*".

- f) The use of CNE to weaken software or hardware at its source, prior to its deployment to users.

This is neither confirmed nor denied.

- g) The obtaining of information for the purpose of maintaining or further developing the intelligence services' CNE capabilities.

This is neither confirmed nor denied.

10. The List of Issues, shorn of its paragraph 6 in which the above matters (a) to (g) were canvassed, appears as Appendix I to this Judgment. We turn to address those issues below, although not quite in the same format.
11. The value of these proceedings in open court before us has been to our mind again emphasised, whatever the outcome, by virtue of the full inter partes consideration of such issues, and in particular:
 - i) The knock-on effect that the very existence of these proceedings has clearly had. We have already noted the fact that the publication of the draft E I Code was on 6 February 2015, revealing for the first time in public the use by GCHQ of CNE and the procedures under which it is

to operate (in particular at paragraph 1.9 "*Equipment Interference is conducted in accordance with the statutory functions of each Intelligence Service*"). That was the same date as the service of the Respondents' Open Response in these proceedings, setting out their case as to CNE. The Claimants have pointed to the fact that within a month after the initiation in May 2014 of these proceedings by Privacy International, by which the Claimants raised the issue as to the import of s.10 of the Computer Misuse Act 1990 ("CMA"), proposed amendments to s.10 were laid before Parliament on 5 June 2014 (as part of the Serious Crime Bill), which have now been enacted. These amendments are said by the Respondents to clarify, but asserted by the Claimants to change, the nature of the un-amended s.10, which forms the basis of the discussion in Issue 1 below, and plainly were also a consequence of these proceedings.

- ii) There are now in the public domain what were previously "*below the waterline*" arrangements (see paragraph 7 in the Liberty/Privacy No.1 judgment) underlying both the Property Code and the E I Code, either redacted or gisted. Whether or not in the event they are determinative in relation to the issues canvassed before us in relation to the question of accessibility or foreseeability under Articles 8 and 10 of the ECHR, it is valuable that they have been produced by the Respondents in these proceedings. This arose as a result of the disclosure sought by the Claimants, and by Counsel to the Tribunal, and requested by the Tribunal.
- iii) Simultaneously with the preparation and eventual presentation of this case, there has been the consideration by David Anderson QC, the Independent Reviewer of terrorism legislation, in his Report dated June 2015, and subsequently the draft Investigatory Powers Bill ("the IP Bill") laid before Parliament in November 2015, which in its present form has been before us, both of which plainly drew upon the ideas and submissions which have now been openly canvassed before us.

Issue 1: s.10 CMA

- 12. The first Issue is: Was an act which would be an offence under s.3 of the CMA made lawful by a s.5 warrant or s.7 authorisation, prior to the amendment of s.10 CMA as of May 2015?
- 13. The following is common ground:
 - i) S.1 of CMA reads in material part as follows:

"1. Unauthorised access to computer material.

(1) A person is guilty of an offence if—

 - (a) he causes a computer to perform any function with intent to secure access to any program or data held in any*

computer, or to enable any such access to be secured;

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

..."

ii) S.3 reads as follows:

"3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if -

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act -

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) to (c) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section -

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

..."

- iii) An act of CNE, insofar as it consists of, for example, removing or replacing information on a computer, would not simply constitute an offence under s.1 but plainly also under s.3 (unless exempt from sanction).
- iv) Since 3 May 2015 the amendment to s.10 (referred to in paragraph 11(i) above) makes it clear that a person acting under a s.5 warrant or s.7 authorisation commits an offence neither under s.1 nor under s.3 of the CMA.

So the only issue relates to the period prior to 3 May 2015.

14. S.10 of the CMA prior to its amendment read as follows:

"10. Saving for certain law enforcement powers

Section 1(1) above has effect without prejudice to the operation –

(a) In England and Wales of any enactment relating to powers of inspection, search or seizure; and

(b) In Scotland of any enactment or rule of law relating to powers of examination, search or seizure.

...”

15. S.10 as amended by the Serious Crime Act 2015 s.44(2)(a) now reads as follows:

“10. Savings

Sections 1 to 3A have effect without prejudice to the operation -

(a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure or of any other enactment or rule of law by virtue of which the conduct in question is authorised or required.

and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of any of those sections. In this section—

“enactment” means any enactment, whenever passed or made, contained in—

(a) an Act of Parliament;

(b) an Act of the Scottish Parliament;

(c) a Measure or Act of the National Assembly for Wales;

(d) an instrument made under any such Act or Measure;

(e) any other subordinate legislation (within the meaning of the Interpretation Act 1978)

...”

16. The Claimants submit that until the passage of this amendment to s.10 any act of CNE which would contravene s.3 of the CMA was unlawful. On the Claimants' case, the effect of the amendment is to reverse the previous position; hence the need for it. The Respondents submit however that the amendment to s.10 was simply clarificatory. This the Respondents submit was made clear by the Home Office Circular (Serious Crime Act 2015) and the Home Office Fact sheet, both dated March 2015, which accompanied the bill. It is not contested that such documents are admissible in construction of

the bill which they accompanied, but it is equally accepted that those documents cannot provide any aid to construction of the original 1990 CMA.

17. Mr Jaffey submits that:

- i) The CMA is the '*lex specialis*' relating to computer misuse. It governs the position, and there is specific reference in the unamended s.10 to the law enforcement powers which are exempted from the ambit of s.1, and s.3 is left entirely unaffected. When the ISA was enacted in 1994, it could not affect the position, namely that it is only s.1 of the CMA which has effect "*without prejudice to the operation in England and Wales of any enactment relating to powers of inspection, search or seizure*", and not s.3
- ii) There may be good reason for Parliament having so differentiated because:
 - (a) Parliament is to be taken to have decided that less intrusive operations would be exempted from the ambit of the Act and not the more excessive activity covered by s.3.
 - (b) It may be that there were concerns that an act which would contravene s.3 might impact upon the reliability of evidence contained in a computer, in the context of its being admitted into evidence in subsequent criminal proceedings (there being no bar on the admission of such evidence, as there is and was in relation to intercept evidence). There is some discussion in **Hansard** at the time of passage of the bill as to concerns about the position of such evidence.
- iii) The 1990 CMA, and its express savings, cannot be impliedly overruled by the subsequent 1994 ISA (see Lord Hope in **H v Lord Advocate** [2013] 1 AC 413 at 436, paragraph 30 as to implied subsequent repeal).

18. Mr Eadie submits that:

- i) The language of ss.5 and 7 of the ISA, set out in paragraph 4 above is in each case clear. No act done pursuant to those sections can be unlawful either civilly or criminally. That plainly includes an act which would otherwise be an offence under s.3 of the CMA.
- ii) The 1994 ISA was the '*lex specialis*' relating to the Intelligence Agencies. Earlier savings provisions cannot limit the powers given under s.5 and s.7 of ISA. S.10 of CMA (as un-amended) did not purport to be exhaustive: the heading, which is admissible for interpretation, refers to "*saving for certain law enforcement powers*", and even the words "*any enactment relating to powers of inspection, search or seizure*" would only appear to be relevant in relation to s.1 of CMA and not necessarily to s.3. In any event s.5 and s.7 post-date the CMA, and expressly authorise and exempt from sanction the relevant conduct, and it would be unthinkable that acts under it, in accordance

with GCHQ's express powers under s.3(1)(a), would be unlawful. Ss.5 and 7 are not, and are not relied upon as, an implied repeal of what was only a savings clause in the 1990 Act.

iii) With regard to the 1990 discussion in **Hansard**, there is no sign that concerns about the admissibility of evidence were discussed in the specific context either of s.3 or of (what became) s.10. In any event it is plain from **Hansard** that there was an amendment put forward, which would have placed what was called a temporary stop (pending further debate) preventing the Security Service from misusing computers (this would have been pursuant to s.3 of the 1989 Act referred to in paragraph 6(i) above). This amendment ("to prevent *hacking or similar activities by the Security Service*") was not pressed. It would seem therefore that it was accepted that the 1989 Act, already on the statute book, was not affected by the CMA. *A fortiori* the subsequent 1994 Act is not either.

19. We would add that if reference is made to the definition section in s.17 of the CMA there is not in fact a dramatic difference between *securing access* under s1 and acts covered by s.3 in any event. S.17(2) reads as follows:

"(2) *A person secures access [our underlining] to any program or data held in a computer if by causing a computer to perform any function he*

(a) *Alters or erases the program or data;*

(b) *Copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;*

(c) *Uses it; or*

(d) *Has it output from the computer in which it is held (whether by having it displayed or in any other manner).*

And references to access to a program or data (and to an intent to secure such access . . .) shall be read accordingly."

Any concern about potential impact on computers for subsequent admissibility purposes would be as live in respect of such a wide definition of s.1 as it would be in respect of s.3.

20. Whatever was the purpose lying behind the precise wording of s.10 in its un-amended form, it seems to us clear that it had no effect upon and/or was expressly overtaken by the clear words of ss.5 and 7 of the ISA. It would indeed be extraordinary that proportionate and necessary steps taken for the

(permitted) purpose of protecting national security, taken under an express power under ss.5 or 7 of the ISA, and covered by an express removal of civil or criminal liability, could be rendered unlawful by reference to a saving under an earlier statute. The inability lawfully to take such steps under ss.5 and 7 would render the very function of GCHQ in relation to computers provided for in s.3 of ISA (set out in paragraph 4 above), including powers to “*monitor or interfere with electro magnetic, acoustic and other emissions . . . in the interests of national security*”, entirely nugatory. Any argument in support of such an extraordinary outcome has been removed by the amendment, which is, we are satisfied, simply clarificatory, and we accept Mr Eadie’s submissions.

Issue 2: Territorial jurisdiction in respect of ss.5/7

21. The Issue was: If an act by the Respondents constituting CNE was unlawful prior to May 2015, would any such act abroad have been unlawful?
22. S.4 of the CMA provides that it is immaterial whether any act occurred in the UK or whether the accused was in the UK at the time of any such act, provided that there was “*at least one significant link with domestic jurisdiction*” at the relevant time. By s.5, where the accused was in a country outside the UK at the time of the act constituting the offence, there would be such a significant link with domestic jurisdiction if the accused was a UK national at the time, and the act in question constituted an offence under the law of the country in which it occurred.
23. As we have decided Issue 1 in favour of the Respondents, this issue 2 does not arise. Suffice it however to say that the jurisdictional provisions of ss.4 and 5 of the CMA are very broad, and s.4 (2) provides that: “*at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed*”. The question could therefore only arise if there is no such significant link. Mr Jaffey sought to contend that s.31 of the Criminal Justice Act 1948 would render a Crown servant, such as an employee of GCHQ, criminally liable in such a case because it provides that “*any British subject employed under His Majesty’s Government in the United Kingdom in the service of the Crown who commits, in a foreign country, when acting or purporting to act in the course of his employment, any offence which, if committed in England, would be punishable on indictment, shall be guilty of an offence*”. Although in the event we do not have to answer this issue, it appears clear to us that, in order for s.31 to avail, there would need to have been an offence under the CMA, which there would not have been if there was no *significant jurisdictional link*, and in any event, just as with the CMA itself, there would be the requirement to prove ‘double criminality’. As it is, Issue 2 does not specifically require to be answered, but we conclude that any act abroad pursuant to ss.5 or 7 of the ISA which would otherwise be an offence under ss.1 and/or 3 of the CMA would not be unlawful.

Issue 3: Intangible property

24. Issue 3 as formulated by the parties is: “Does the power under s.5 of ISA to authorise interference with “property” encompass physical property only, or does it also extend to intangible legal rights, such as copyright?”.

25. There is no definition of *property* in s.5 of the ISA. The relevant provision, set out above, simply refers to a warrant "*authorising the taking . . . of such action as is specified in the warrant in respect of any property [our underlining] so specified or in respect of wireless telegraphy so specified*". On the face of it, not only is the definition of property not limited to real or personal property, but there is nothing to exclude intangible property. The definition "*any property*", would appear to include it, and this is emphasised by the inclusion as an alternative subject matter of the warrant of "*wireless telegraphy*".
26. There appear to be two matters which led the Claimants to pursue this argument:
- i) The reference in a document published by Mr Snowden, and exhibited by the Claimants, to there possibly being a s.5 warrant which permitted interference with computer software in breach of copyright and licensing agreements.
 - ii) The reference in s.5(3), and in s.5(3A) (for MI5), to the inapplicability of certain warrants in respect of "*property in the British Islands*". Mr Jaffey said that this is an inapt reference if intangible property is intended. But there appears to us to be no answer either to Mr Beard QC's succinct submissions on this topic for the Respondents, including the point that as defined by statute copyright is a collection of rights in respect of the United Kingdom, or to that put by the Tribunal in relation to choses in action such as bank accounts, which again would have a geographical identity.
27. The whole of this contention seemed to us to evaporate in the course of argument, when Mr Jaffey accepted (Day 1/127, 138, Day 2/14-16) that physical interference with property in the context of CNE authorised by a s.5 warrant may also involve an interference with copyright, which would then be taken to be authorised, as compared with what he called a "*pure interference with intellectual property rights*", i.e. that interference with copyright would be authorised if ancillary to interference with physical property.
28. We can see no justification whatever for such a construction of the Statute. We are satisfied that s.5 extends to intangible property, whether the action is directed at intangible property alone or is ancillary to interference with physical property. We note that this is also the view of the Intelligence Services Commissioner (page 17 of his Report of 25 June 2015). A s.5 warrant is as sufficient authority for such interference as is s.50 of the Copyright Designs and Patents Act 1988, whereby "*where the doing of a particular act is specifically authorised by an Act of Parliament, whenever passed, . . . the doing of that act does not infringe copyright*".
29. An argument in relation to the possible impact of the EU Copyright Directive (2001/29/EC), raised by Mr Jaffey in his pleadings and his skeleton argument, was not pursued.
30. Accordingly we resolve this issue in favour of the Respondents.

Issue 4: "Thematic warrants" and the requirement for specification under s.5

31. We have set down the words "*thematic warrants*" in the above heading, because the words are used in the Agreed Issues. However, not only do such words have no statutory basis, but such description does not appear to us to capture the reality of the issue which we have to decide. The words first appear in a completely different context, namely at page 21 of the ISC Report of 12 March 2015, a passage in which interception warrants under s.8(1) of RIPA were being discussed.

32. S.8(1) provides that:

"(1) An interception warrant must name or describe either -

(a) one person as the interception subject; or

(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place."

The ISC state in their Report in a section under the heading "*Thematic warrants*" as follows:

"42. While the very significant majority of 8(1) warrants relate to one individual, in some limited circumstances an 8(1) warrant may be thematic. The term 'thematic warrant' is not one defined in statute. However, the Home Secretary clarified that Section 81 of RIPA defines a person as "[including] any organisation [and] any association or combination of persons", thereby providing a statutory basis for thematic warrants. The Home Secretary explained that "the group of individuals must be sufficiently defined to ensure that I, or another Secretary of State, is reasonably able to foresee the extent of the interference and decide that it is necessary and proportionate"

43. MI5 have explained that they will apply for a thematic warrant "where we need to use the same capability on multiple occasions against a defined group or network on the basis of a consistent necessity and proportionality case . . . rather than [applying for] individual warrants against each member of the group."

There is then discussion by reference to the issue of a s.8(1) warrant in the context of a number of circumstances where it may be appropriate to grant such a warrant by reference to a group linked by a specific intelligence requirement. The thematic reference is obviously because of the wide coverage of an (otherwise specific) s.8(1) warrant by virtue of the broad definition of '*person*' in s.8(1).

33. The description is taken up by the Intelligence Services Commissioner at paragraph 849 of his 2014 Report at page 18, which reads (though now in the context of a s.5 warrant) as follows:

"Thematic Property Warrants

I have expressed concerns about the use of what might be termed "thematic" property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers "to a particular act" or to "acts" undertaken in the course of an operation. However, section 5 is narrower referring to "property so specified".

During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or "thematic". I have expressed my view that:

- section 5 does not expressly allow for a class of authorisation; and*
- the words "property so specified" might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals.*

The agencies and the warrantry units argue that ISA refers to action and properties which "are specified" which they interpret to mean "described by specification". Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which "specifies" property by reference to a described set of persons, only being able to identify with precision an individual at a later moment.

I accept the agencies' interpretation is very arguable. I also see in practical terms the national security requirement.

The critical thing however is that the submission and the warrant must be set out in a way which allows the

Secretary of State to make the decision on necessity and proportionality."

It is plainly from this passage that Mr Jaffey has drawn the basis for his submissions set out below, and which have led to the formulation of Issue 4.

34. We prefer however to phrase Issue 4 as: What is the meaning of the words 'in respect of any property so specified' for the purposes of the issue of a s.5 warrant?
35. Mr Jaffey submits as follows:
- i) The common law sets its face against general warrants, as is well known from the seminal Eighteenth Century cases such as Entick v Carrington [1765] 2 Wilson KB 275 and Money v Leach [1765] 3 Burr 1742. As for statute law, he relies on Lord Hoffmann in R v Secretary of State for the Home Department, Ex p Simms [2000] 2 AC 115 at 131: "*Fundamental rights cannot be overridden by general or ambiguous words*". Thus he takes as a starting point that such words as were disapproved in the warrant in Money v Leach, relating to searching for and seizing the papers of the authors, printers and publishers of the North Briton (wheresoever found), should not be permitted pursuant to a s.5 warrant, or that a s.5 warrant should not be defined so as to permit "*any property so specified*" to include such a provision.
 - ii) He contrasts the provision in s.5(2) for a warrant "*in respect of any property so specified*" with the authorisation provided for in s.7, only available in respect of *acts outside the British Islands*, which by s.7(4) "*may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified*". This latter is, and was described by the Intelligence Services Commissioner in the passage from his Report quoted above as, a '*class authorisation*'. It relates effectively to any operation carried out abroad by the Agencies: and there is provision within the E I Code (paragraphs 7.11-7.14) for situations where, because "*an authorisation under section 7 may relate to a broad class of operations*" (7.11), "*Where an authorisation relating to a broader class of operations has been given by the Secretary of State under section 7, internal approval to conduct operations under that authorisation in respect of equipment interference should be sought from a designated senior official*"(7.12). Mr Jaffey submits that this emphasises the difference between a s.7 authorisation and a s.5 warrant. The former can authorise a broader class of operation, but is subject to specific subsequent approvals, whereas the latter is not subject to any such protective or limiting provision.
 - iii) Mr Jaffey accepts that the property specified in a s.5 warrant may include a reference to more than one person or more than one place, up to an unlimited number, provided they are properly specified. But he submits that it must not extend to authorising an entire operation or

suite of operations, and that identification cannot depend upon the belief, suspicion or judgment of the officer acting under the warrant. It must also be possible to identify the property/equipment at the date of the warrant. Thus a warrant permitting CNE in respect of computers owned or used by any diplomatic representatives of the State of Ruritania, or by any member of a named proscribed organisation, is not adequate because (i) who they are is thus left open (unless a list of names is provided to be attached to the warrant); (ii) it is not limited to those who are part of that group at the time of the warrant; (iii) it leaves too much to the belief, suspicion or judgment of the officer, and deprives a Secretary of State of the opportunity to exercise his required discretion as to the necessity and proportionality of the warrant. Mr Jaffey submitted (Day 2/12) that the Secretary of State had to consider before granting a warrant whether or not such intrusion would be justified in the case of each individual.

- iv) Mr Jaffey had made reference to **Hansard** in respect of discussion in Parliament in 1989, prior to the passage of the Security Service Act 1989, but both parties agreed that this was of no assistance. However Mr Jaffey also referred to the IP Bill, referred to in paragraph 11(iii) above, for the purpose of showing what is now proposed, by reference to clause 83 in Part 5 of the Bill. The IP Bill provides, by clause 81, for a new warrant, to be called a "*targeted equipment interference warrant*", and the broad definition of the subject matter of such proposed warrant is set out in clause 83, including eight permitted such targets including, by way of example "*(a) equipment belonging to, used by or in the possession of the particular person or organisation*" and "*(b) equipment belonging to, used by or in the possession of persons who form a group that shares a common purpose or who carry on, or maybe carrying on, a particular activity*". His submission is that such defined targets are much wider than what he submits is the more limiting ambit of a s.5 warrant.

36. Mr Eadie responds as follows:

- i) As to the Eighteenth Century common law cases, they are at best of marginal relevance. They plainly relate to the limitation on common law powers in relation to executive acts within the United Kingdom. S.5 is not limited to acts within the United Kingdom and in any event is a creature of statute. The legislative context and intent relate to the powers of the Secretary of State in respect of the protection of national security, and substantial limitation is imposed by the requirement of the section itself to consider whether the warrant falls within the statutory purposes of the agency applying for it (s.3(1) so far as concerns GCHQ) ("legality"), necessity and proportionality. The word "*specified*" is used three times in s.5(2), relating to the actions sought to be authorised and in respect of any property or "*wireless telegraphy*". He submits that what is required is the best description possible. Even a s.8(1) warrant under RIPA, which is expressly more limited, can have a broad ambit, as discussed in paragraph 32 above,

and the inclusion of “wireless telegraphy” in the section is significant, being very broadly defined (see s.11(e) of the ISA) by reference to what was then the Wireless Telegraphy Act 1949 (now 2006), and, as Mr Jaffey accepted, could extend to an entire communications frequency or a group of communications frequencies.

- ii) S.7 is a different provision. It relates to the “*Authorisation of acts outside the British Islands*”, and is not in direct contrast with, or alternative to, s.5 (in the way for example that s.8(1) and s.8(4) fall to be contrasted in RIPA). Mr Jaffey accepts that a s.5 warrant can extend to property owned or used by a group of persons, and there may therefore be occasions in which the scope of a s.5 warrant may cover similar conduct to an operation which, if overseas, could be sanctioned under s.7, but it is nevertheless directed at specified property. Only in 2001 was s.7 amended so as to add the power for GCHQ to seek a s.7 authorisation, by the Anti-terrorism, Crime and Security Act 2001. Until then GCHQ could only rely on s.5. Thus in any event there was no such contrast between s.5 and s.7 so far as concerned GCHQ at the date of the passage of the Act.
- iii) Mr Eadie does not accept any of the limiting propositions set out in paragraph 35(iii) above. He submits that the requirement is for the actions and property to be objectively ascertainable. The examples referred to above, both as to Ruritania and proscribed organisations, are in his submission entirely proper and adequate. It is not necessary to identify persons any more than is possible at the time of the issue of the warrant, and it is certainly not necessary for the individuals to be identified by name or by reference to the particular time when the warrant is issued. A warrant could cover, in the examples given, anyone who was at any time during the duration of the warrant (six months unless specifically renewed) within the defined group. What is important is that an application for a warrant contains as much information as possible to enable a Secretary of State to make a decision as to whether to issue a warrant, and, if so, as to its scope. This might involve reducing or putting a limit on the persons or category of persons covered, or defining property by reference to such a restriction. He submits that what is fundamental is the duty imposed on the Secretary of State to consider whether the warrant is within the powers of the agency applying for it (legality) and whether the issue of the warrant would satisfy the tests of necessity and proportionality. That is the discipline referred to in paragraph 88 of R (Miranda) -v- Secretary of State for The Home Department [2014] 1 WLR per Laws LJ.¹ Mr Jaffey points out that the requirement for proportionality was not introduced into s.5 by amendment until after the introduction of the Human Rights Act 2000, by the passage of RIPA, and that it cannot have been intended thereby to alter the scope of a lawful warrant under s.5. Mr Eadie points to the words of Lord Toulson in R

¹ The decision in the Court of Appeal ([2016] EWCA Civ.6), subsequent to the hearing before us, does not question the importance of this discipline, but considers the overlay of Article 10 in relation to press freedom (per Lord Dyson MR at paras 98-117).

(Brown) v Secretary of State for the Home Department [2015] UKSC 8 at paragraph 24, as to the relevance of a subsequent amendment to interpretation of the statute. In any event he is content to rely if necessary on the duties of the Secretary of State as to legality and necessity already, as he puts it, "*hard-wired*" into s.5 prior to 2000. He submits that the words of the North Briton warrant, referred to in paragraph 35(i) above, would, subject to questions of necessity and proportionality in the particular circumstances, certainly be sufficiently specified. Another example canvassed in the course of the hearing was "*all mobile phones in Birmingham*". This could, submitted Mr Eadie, be sufficiently *specified*, but, save in an exceptional national emergency, would be unlikely to be either consistent with necessity or proportionality or with GCHQ's statutory obligations.

iv) Mr Eadie submits that (as is indeed said in its accompanying Guide) the IP Bill, albeit in respect of a differently named warrant, brings together powers already available, and the descriptions of targets in the new proposed clause 83 would, subject to the requirements of necessity and proportionality, all be consistent with the existing s.5.

37. We accept Mr Eadie's submissions. Eighteenth Century abhorrence of general warrants issued without express statutory sanction is not in our judgment a useful or permissible aid to construction of an express statutory power given to a Service, one of whose principal functions is to further the interests of UK national security, with particular reference to defence and foreign policy. The words should be given their natural meaning in the context in which they are set.

38. The issue as to whether the specification is sufficient in any particular case will be dependent on the particular facts of that case. The courts frequently have to determine such questions for example in respect of a warrant under the Police Act 1997 s.93, when the issues, by reference to the particular facts would be fully aired in open. That is not possible in relation to a s.5 warrant, but it may still be subject to scrutiny by the Intelligence Services Commissioner, by the ISC and, if and when a complaint is made to this Tribunal, then by this Tribunal. But the test is not in our judgment different - Are the actions and the property sufficiently identified? The Home Secretary's own words as recorded in paragraph 42 of the ISC Report, set out in paragraph 32 above, relating to a s.8(1) warrant, are applicable here also. It is not in our judgment necessary for a Secretary of State to exercise judgment in relation to a warrant for it to be limited to a named or identified individual or list of individuals. The property should be so defined, whether by reference to persons or a group or category of persons, that the extent of the *reasonably foreseeable interference* caused by the authorisation of CNE in relation to the actions and property specified in the warrant can be addressed.

39. As discussed in the course of argument, the word under consideration is simply *specified*, and this may be contrasted with other statutes such as those relating to letters of request, where the requirement of the Evidence (Proceedings in Other Jurisdictions) Act 1975 is for "*particular documents specified*". There is no requirement here for specification of *particular*

property, but simply for specification of the property, which in our judgment is a word not of limitation but of description, and the issue becomes one simply of sufficiency of identification.

40. The statute does not fall to be interpreted by reference to the underlying Code, in particular one which, like the E I Code, has been in draft waiting to be approved by Parliament. But what is of course important is what is put in the applications to the Secretary of State, so that he can exercise his discretion lawfully and reasonably. Both in the Property Code, in place since 2002, (at paragraphs 7.18-7.19) and now in the E I Code (at paragraph 4.6), there is a lengthy list of what is required to be included in an application to the Secretary of State for the issue or renewal of a s.5 warrant. Apart from a description of the proposed interference and the measures to be taken to minimise intrusion, at the head of the list in both Codes is a requirement to specify "*the identity or identities, where known, of those who possess [or use] the [equipment] that is to be subject to the interference*" and "*sufficient information to identify the [equipment] which will be affected by the interference*" (the square bracketed parts are the changes from the Property Code to the draft E I Code).
41. We are entirely satisfied that Mr Jaffey's submissions have confused the property to be specified with the person or persons whose ownership or use of the equipment may assist in its identification. We do not accept his submission (Day 2/12) that the Secretary of State has to consider, by reference to each individual person who might use or own such equipment, whether CNE would be justified in each individual case. Questions of necessity and proportionality to be applied by the Secretary of State must relate to the foreseeable effect of the grant of such a warrant, and one of the matters to be considered is the effect and extent of the warrant in the light of the specification of the property in that warrant.
42. As originally enacted, s.5(2) authorised the Secretary of State to issue a warrant "*authorising the taking . . . of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State:*
 - (a) *thinks it necessary for the action to be taken on the ground that it is likely to be of substantial value in assisting ... [our underlining]*
 - (iii) *GCHQ in carrying out any function which falls within Section 3(1)(a) and*
 - (b) *is satisfied that what the action seeks to achieve cannot reasonably be achieved by other means and*
 - (c) *is satisfied that satisfactory arrangements are in force under ... Section 4(2)(a) above with respect to the disclosure of information obtained ... and that any information obtained under the warrant will be subject to those arrangements*".
43. "*Specified*" must mean the same in relation to each action, property and wireless telegraphy. "*Wireless telegraphy*" as defined by s.11(e) of ISA meant

“the emitting or receiving over paths which are not provided by any material substance constructed or arranged for that purpose, of electro magnetic energy or frequency not exceeding 3 million megacycles per second . . .”. (S.19(1) Wireless Telegraphy Act 1949).

44. Given the width of meaning contained in the words “action” and “wireless telegraphy” and, at least potentially, in the word “property”, *specified* cannot have meant anything more restrictive than ‘adequately described’. The key purpose of specifying is to permit a person executing the warrant to know when it is executed that the action which he is to take and the property or wireless telegraphy with which he is to interfere is within the scope of the warrant.
45. It therefore follows that a warrant issued under s.5 as originally enacted was not required:
- i) to identify one or more individual items of property by reference to their name, location or owner or
 - ii) to identify property in existence at the date on which the warrant was issued.

Warrants could therefore, for example, lawfully be issued to permit GCHQ to interfere with computers used by members, wherever located, of a group whose activities could pose a threat to UK national security, or be used to further the policies or activities of a terrorist organisation or grouping, during the life of a warrant, even though the members or individuals so described and/or of the users of the computers were not and could not be identified when the warrant was issued.

46. The amendment of s.7 in 2001 to add GCHQ cannot alter the meaning of s.5, which has, in all respects relevant to this Issue, remained unchanged.
47. In our judgment what is required is for the warrant to be as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable.

Issue 5: Scope of the Convention

48. Issue 5 is the question: Do Articles 8/10 apply to a complaint by reference to a s.7 authorisation? This issue only arose specifically in the course of the hearing, in which the Tribunal is of course being asked to decide pursuant to the List of Issues whether *“the regime which governs [CNE] is ‘in accordance with the law’ under Article 8(2) ECHR ‘prescribed by law’ under Article 10(2) ECHR”* (original Legal Issue 4).
49. S.7 applies, as is clear from its heading, to *“authorisation of acts outside the British Islands”*. S.7 was not dealt with in the Property Code, and there is no power for the Secretary of State to issue Codes of Practice in relation to s.7, by

reference to s.71 of RIPA or at all (see paragraph 1.4). In that paragraph, and more specifically in paragraph 7.1 of the E I Code, it is stated that "*SIS and GCHQ should as a matter of policy apply the provisions of [the] code in any case where equipment interference is to be, or has been, authorised pursuant to section 7 of the 1994 Act in relation to equipment located outside the British Islands*". But there is a footnote to that paragraph which expressly says "*without prejudice as to arguments regarding the applicability of the ECHR*".

50. It was, in the event, common ground that, subject to Mr Jaffey's reserving his clients' position to be considered further if necessary in the ECtHR, there is a jurisdictional limit on the application of the ECHR, by virtue of Article 1, ECHR, which provides that "*the High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section 1 of this Convention*". It was also common ground that, in the absence of any ECtHR authority, the Convention should not be interpreted more generously in favour of claimants than the ECtHR has been prepared to go, in circumstances where there is no right of appeal for the Government from the domestic courts to the ECtHR: see **R (Ullah) v Secretary of State for the Home Department** [2004] 2 AC 323 at para 20 per Lord Bingham.
51. Jurisdiction under the ECHR is accordingly territorial; and it is only in exceptional circumstances that extraterritorial jurisdiction arises (see **Banković v UK** [2007] 44 EHRR SE 5 and **Al-Skeini v UK** [2011] 53 EHRR 18 at para 131). As is made clear in **Banković** at paragraph 73, jurisdiction is not a doctrine of 'mere effects'.
52. There is thus no dispute between the parties that in ordinary circumstances there would be no jurisdiction by reference to Articles 8 or 10 with regard to the acts outside the British Islands which would be the subject of authorisation under s.7. Mr Eadie submitted that other circumstances would be exceptional. Mr Jaffey gave examples of circumstances which might engage those Articles: complainant in the jurisdiction but computer or information abroad, computer or phone brought back to the jurisdiction etc. But he accepted that in most cases where someone who is the subject of an authorisation granted under s.7 is abroad it was difficult to argue that such person is within the territorial scope of the Convention, and in any event that there would be a "*very limited number of circumstances*" in which there was going to be a breach of the Convention (Day 2/25). As is clear from the current Advance Training for Active Operations, disclosed in these proceedings, "*CNE operations must be authorised under ISA Section 5 or Section.7, depending whether the target computer or network is located within or outside the British Islands*".
53. Before fully accepting the consequences of the jurisdiction argument, which the Vice-President had put to him, Mr Jaffey appeared to argue (Day 1/161) that any s.7 authorisation prior to the introduction of the E I Code "*had to fall*" (Day 1/161), a submission which he later expressly clarified (Day 3/177). Both in that latter passage and earlier (Day 2/24-26) he appeared to agree in clear terms with Mr Eadie (Day 3/120) that the fact that there might be an individual claimant who might be able to claim a breach of Article 8/10 rights as a result of a s.7 authorisation would not lead to a conclusion that the s.7 regime as a whole could be argued to be non-compliant with Articles 8 or 10.

In any event we reserve for future consideration, if and when particular facts arise and the position of jurisdiction to challenge a s.7 warrant can be and has been fully argued, whether an individual complainant may be able to mount a claim. Even though Issue 5 was formulated as an agreed preliminary issue between the parties, it is clear to the Tribunal that, given the agreed difficult issues as to jurisdiction, we have an insufficient factual basis, assumed or otherwise, to reach any useful conclusion.

Issue 6: A s.5 warrant and Articles 8/10

54. We have concluded in respect of Issue 4 that a s.5 warrant is not as restricted as the Claimants have contended, by reference to construction of it at domestic law. Mr Jaffey submits that the Respondents are on a Morton's Fork, and that the wider the construction of s.5 for which they contend the more unlikely it is that there will be sufficient safeguards for the purposes of the ECHR. We can deal with this issue quite shortly.
55. Part of Mr Jaffey's case is again that, whereas s.7 provides for underlying approvals, as referred to in paragraph 35(ii) above, s.5 does not. But the essential question is, if an application for a warrant so specifies the property proposed to be covered by it as to enable a Secretary of State to be satisfied as to its legality, necessity and proportionality, and so that the property to be covered is objectively ascertainable (paragraph 47 above), whether a warrant so issued is in adequate compliance with the Convention.
56. As to Mr Jaffey's submissions in this regard:
- i) He refers to **Malone v UK** [1985] 7 EHRR 14 as his foundation, but in that case, as he reminded us, the ECtHR made clear that "*in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations*" long before the present suite of statutory provisions. What the Court laid down as fundamental requirements, as set out in paragraphs 67 and 68 of the Judgment, is that "*there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities . . . A law which confers a discretion must indicate the scope of that discretion*".
 - ii) He naturally referred to **Weber** and **Saravia v Germany** [2008] 46 EHRR SE5, which we addressed in detail in **Liberty/Privacy (No.1)**, and in paragraph 33 of that judgment we set out the "**Weber** requirements", numbering them from 1 to 6 for convenience:

"95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the

data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed."

57. In R.E. v UK, the ECtHR was satisfied, with regard to the surveillance provisions there referred to, so far as concerned Weber (1) and (2) at paragraph 136 of its Judgment, and so far as duration is concerned gave approval in paragraph 137. Duration of the s.5 warrant is limited by s.6, to which no specific criticisms have been addressed.
58. In Weber itself, a broad and untargeted warrant, similar to a warrant under s.8(4) of RIPA - a far broader and less *specified* warrant than the s.5 warrant which we are here considering - was found to comply with the Convention.
59. We are satisfied in this case that a s.5 warrant which accords with the criteria of specification which we have set out at paragraph 47 above complies with Weber (1) to (3), namely in regard to the circumstances, the definition of the categories of people/property and duration, and consequently with Articles 8 and 10 in that regard. We deal with Weber (4) to (6) below.

Issue 7: Bulk CNE

60. Issue 7 relates to the absence of a similar certificate to that in s.16 of RIPA in relation to CNE. It arises from the matters in (e) in the original paragraph 6 of the List of Issues, set out in paragraph 9 above, which were the subject of NCND by the Respondents. There are two specific complaints which are made:
 - i) That, unlike in the case of a s.8(4) warrant under RIPA, where communications are intercepted in bulk and subsequently accessed for examination, there is no provision, in the event of this occurring pursuant to CNE, for 'filtering': i.e. as in s.16(1) and (3) of RIPA for intercept to be read, looked at or listened to only by reference to a certificate that the examination of material selected is necessary for one of the statutory purposes. S.16 is what was referred to in Liberty/Privacy (No.1) (paragraph 103) as the provision which did the 'heavy lifting'.
 - ii) That there is no special protection, if information is obtained in bulk through the use of CNE, for those persons *known to be for the time being in the British Islands*, as in s.16(2)(3) and (5) of RIPA. Such a scenario is in fact addressed in the E I Code at paragraph 7.4 (relating to a s.7 warrant) which reads:

"7.4 If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation

authorised under section 7. In the event that any equipment located overseas is brought to the British Islands during the currency of the section 7 authorisation, and the act is one that is capable of being authorised by a warrant under section 5, the interference is covered by a 'grace period' of 5 working days (see section 7(10) to 7(14)). This period should be used either to obtain a warrant under section 5 or to cease the interference (unless the equipment is removed from the British Islands before the end of the period)."

David Anderson in his Report refers to this paragraph of the E I Code, and comments, at paragraph 6.33:

"It does not elaborate on what factors should be taken into account in the course of that 'consideration'."

61. As for the latter point (ii), Mr Eadie submits, and we accept, that, provided that the matter is indeed considered, as is required by paragraph 7.4, such an issue is simply one of the matters which are required to be brought before a Secretary of State, pursuant to his obligation to consider alternative and/or less intrusive measures, rather than, as Mr Jaffey submitted, that this is part of an attempt to circumvent the statutory scheme under s.8(4).
62. Both aspects of Mr Jaffey's complaints appear to have been taken up in the IP Bill. Under the heading "*BULK POWERS*" in the accompanying Guide, it is stated, at paragraph 42, that where the content of a UK person's data, acquired under bulk interception and bulk equipment interference powers, is to be examined, a targeted interception or equipment interference warrant will need to be obtained. As for the question of presence in the British Islands, it is specifically provided in draft clause 147, within the Chapter dealing with "*Bulk Equipment Interference Warrants*", namely by clause 147(4), that there is to be a similar safeguard to that in s.16 of RIPA in relation to the selection of material for examination referable to an individual known to be in the British Islands at the time.
63. It seems to us clear that these criticisms are likely primarily to relate to Bulk CNE carried out, if it is carried out at all, pursuant to a s.7 authorisation (hence paragraph 7.4 of the E I Code). Mr Jaffey's own example was of the hacking of a large internet service provider in a foreign country, and the diversion of all of the data to GCHQ, instead of intercepting that material "*over a pipe*" which might be encrypted, so as to render access by ordinary bulk interception difficult if not impossible. As with Issue 5, Mr Jaffey specifically accepted (Day 2/46) that, if Bulk CNE were taking place, and if, prior to any changes such as discussed above, there were to be insufficient safeguards in place, that does not render the whole CNE scheme unlawful. As with Issue 5, we reserve for consideration, on particular facts and when questions of jurisdiction are examined, whether an individual complainant might be able to mount a claim.

Issue 8: S.5 post-February 2015 (Weber (4) to (6))

64. Issue 8 is: Whether the s.5 regime is compliant with the Convention since February 2015. We now address Weber (4) to (6). The E I Code applies to both s.5 and s.7 (see paragraph 49 above), and, as Mr Jaffey accepted, the Respondents, having publicly accepted that they are acting and will act in accordance with the draft Code, are as a matter of public law bound by the Code both in relation to s.5, during the period prior to its being finally approved by Parliament (see paragraph 7 above), and s.7. However in the light of our conclusions in respect of Issue 5, we now address only the question of s.5, though in relation to this Issue the answer would be the same in respect of s.7.
65. We do not need to repeat all of what we said in Liberty/Privacy (No.1) (in particular at paragraphs 38-41) by way of summary of the ECtHR jurisprudence. It suffices to cite what we said at paragraph 41(d), namely:

“It is in our judgment sufficient that:

- i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it . . .*
- ii) They are subject to proper oversight.”*

The oversight relevant to this issue by the Intelligence Services Commissioner seems to us to have been admirable in its dedication to raising any questions of concern.

66. In addition to the E I Code, in November 2015 there was disclosure during these proceedings of *below the waterline arrangements* applicable to GCHQ, whose existence is highlighted in the E I Code (e.g. at paragraph 64) and in statute, as canvassed in our judgments in Liberty/Privacy No.1 and No.2. Insofar as those *arrangements* add something new which had not been previously signposted, and which would not therefore have been *accessible/foreseeable*, then any unlawfulness in relation to the published code would only have been made good by the publication of such *arrangements* in November. Mr Jaffey has submitted that the *arrangements* should have been disclosed earlier, but, as will appear, we do not conclude that the content of those *arrangements* as now disclosed adds anything material to the previously published Code.
67. There has been no material addition to ECtHR jurisprudence since Liberty/Privacy with the exception of R.E. v UK, to which we shall return below, and in which (particularly at paragraph 133) the Court repeated the same principles in the context of national security.
68. It is common ground that compliance with the Convention can be addressed by reference to the Weber requirements, and in this regard specifically by Weber (4) to (6). The significant paragraphs of the E I Code relating to Weber (4) to (6) are in Sections 5 and 6, which are attached as Appendix II to

this judgment, though Weber (6) may not be directly applicable to the use of CNE so far as it consists of 'implants'. We have attached the paragraphs in the form in which they were put before Parliament in November 2015. Although there have been some changes in the draft E I Code during the period of public consultation, and the parties helpfully provided us with tracked changes to explain them, there were none which appeared to us to be material: Mr Jaffey pointed to a number of changes (two in the Sections included in Appendix 2, one in paragraph 6.2 and one in 6.5) of the words *must* to *should*, but he was not able to identify to us, and nor can we see, any material difference in that regard. There are then the *below the waterline arrangements* which have been disclosed from GCHQ's policies, relating to storage of and access to data, and handling/disclosing/sharing of data, obtained by CNE operations. Neither Mr Eadie nor Mr Jaffey suggested that there were any apparent lacunae or alleged inadequacies in the Code which were made good by the disclosure of these *arrangements*.

69. There were very limited criticisms made by Mr Jaffey, in the context of Weber (4) to (6), of the E I Code (even without the supplementary *arrangements*):
- i) He was critical of the apparent lack of provision for record keeping in relation to intrusions pursuant to s.7, but, quite apart from the fact that this related to s.7 and not to s.5, in fact it is clear that, as indeed he accepted, a combination of paragraphs 5.1 and 7.2 of the E I Code does require the keeping of records in relation to "*the details of what equipment interference has occurred*".
 - ii) He described as "*Delphic*" a reference in Mr Martin's witness statement to the nature of a recommendation by the Intelligence Services Commissioner with regard to a s.5 record, but accepted the explanation provided by Mr Eadie during the course of his submissions: Day 3/74.
70. We have no doubt at all that, insofar as compliance must be shown with Weber (4) to (6), the E I Code does so comply, and has so complied since its publication in 6 February 2015, since which time it has been binding in law on the Respondents. We are satisfied that the requirements for records are sufficient and satisfactory, and that adequate safeguards have been in place at all times for the protection of the product of CNE, and that there exists a satisfactory system of oversight.

Issue 9: S. 5 prior to February 2015

71. The issue is: Did the s.5 regime prior to February 2015 accord with the Convention (it is accepted that, as set out in paragraph 49 above, the Property Code did not apply to s.7)?
72. This is obviously a more difficult question, because, by definition, if the publication of the E I Code in February 2015 improved the position, and made sufficiently public the arrangements which govern the use by the Respondents of their powers, the published arrangements prior to February must have been

inferior. Mr Eadie emphasises that the Tribunal, and indeed any court, should not discourage improvement by immediately concluding that what was in existence prior to an improvement was defective. He obviously accepts our conclusion at paragraph 23 of Liberty/Privacy No.2 that, before the disclosures prior to and in our judgment in that case, the regime governing information sharing under Prism had been unlawful, but he submits, as is the case, that there had been effectively no disclosure at all prior to that of the existence of any arrangements, adequate or otherwise.

73. The question for us is, as it was for the ECtHR in Liberty v UK [2008] 48 EHRR 1 (at paragraph 69), whether at the time the regime complied, and that time in these proceedings is, pursuant to the agreed List of Issues at paragraph 4(d), 1 August 2009. The Property Code was in existence throughout the period from August 2009 to February 2015 and did not materially change, and so we have addressed the most recent version (2014).
74. There are underlying issues:
- i) It was not, at any rate with any great force, sought to be argued by Mr Jaffey that the position was any different in relation to Weber (1) to (3) prior to and subsequent to February 2015, and we are satisfied that our conclusions in Issue 6 above apply prior to February 2015, and we shall address for the purposes of this Issue only Weber (4) to (6).
 - ii) It was common ground before us that Weber (1) to (6) constitute a minimum to be complied with, but that there are other factors to consider such as:
 - a) The existence and standard of oversight. It is entirely clear to us that both sides have relied upon his Reports, and that the oversight by the Intelligence Services Commissioner has been of great value.
 - b) The existence of sufficiently signposted underlying *arrangements*, which are adequate to control arbitrary action by the Respondents. It is important to bear in mind, for example, that the Tribunal concluded in Liberty/Privacy No.1 that the s.8(4) regime complied with the Convention, after taking into account the *arrangements*, which we concluded had been adequately signposted prior to any further disclosures by the Respondent (e.g. paragraph 140). This did not involve or require disclosure of the detail of those *arrangements*.
 - iii) R.E. v UK requires to be addressed specifically, as the only relevant ECtHR decision since Liberty/Privacy. The Court was addressing the Property Code (there called the "Revised Code"), and contrasting it with the Interception of Communications Code of Practice ("the Interception Code"), which the ECtHR had approved in Kennedy v UK [2011] 52 EHRR 4. The case before it concerned the issue of the safeguarding of legally and professionally privileged ("LPP") communications in relation to covert surveillance. The Court

concluded that Weber (1) to (3) were satisfied, but that Weber (4) to (6) were not. We shall need to address that conclusion, unfavourable to the Respondents, by the Court.

75. The material provisions for consideration in respect of the period from August 2009 to February 2015 are as follows:

- i) The statutory provision in relation to GCHQ, which is obviously fundamental. This appears in s.4 of ISA.

"4 The Director of GCHQ.

(1) The operations of GCHQ shall continue to be under the control of a Director appointed by the Secretary of State.

(2) The Director shall be responsible for the efficiency of GCHQ and it shall be his duty to ensure—

(a) that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings; and

(b) that GCHQ does not take any action to further the interests of any United Kingdom political party.

...

(4) The Director shall make an annual report on the work of GCHQ to the Prime Minister and the Secretary of State and may at any time report to either of them on any matter relating to its work."

There is a cross reference to s.4 in s.5(2)(c) of ISA, set out in paragraph 4 above together with s.6, which is also relevant.

- ii) The other related statutory provisions set out in paragraph 6(ii), (iii) and (iv) above: disclosure or use by an employee of GCHQ of information in breach of a relevant *arrangement* within s.4(2)(a) of the ISA above set out would constitute a criminal offence pursuant to the OSA.

- iii) The Property Code, being the published *arrangements*. Relevant to Weber (4) to (6) are:

"8.3 The following information relating to all authorisations for property interference should be centrally retrievable for at least three years:

- the time and date when an authorisation is given;
- whether an authorisation is in written or oral form;
- the time and date when it was notified to a Surveillance Commissioner, if applicable;
- the time and date when the Surveillance Commissioner notified his approval (where appropriate);
- every occasion when entry on or interference with property or with wireless telegraphy has occurred;
- the result of periodic reviews of the authorisation;
- the date of every renewal; and
- the time and date when any instruction was given by the authorising officer to cease the interference with property or with wireless telegraphy.

...

9.3 Each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

...

9.7 The heads of these agencies are responsible for ensuring that arrangements exist for securing that no information is stored by the authorities, except as necessary for the proper discharge of their functions. They are also responsible for arrangements to control onward disclosure. For the intelligence services, this is a statutory duty under the 1989 Act and the 1994 Act.”

76. There are then the *under the waterline* arrangements. In this regard we refer to paragraphs 42 to 44 of the Tribunal’s judgment in **Liberty/Privacy No.1**, the relevant cross-references for the purposes of this case being to paragraph 18(ix) and (xi) of that Judgment. In addition to the statutory provisions we have referred to in paragraph 75 above, there is the reference in paragraph 9.3 of the Property Code to *arrangements* and *codes of practice*. The arrangements so signposted are summarised in paragraph 99ZK-99ZR of the

Respondents' Open Response as follows (underlining in the original signifies the existence of gisting):

"Storage of and access to data

99ZK. *GCHQ also has policies for storage of and access to data obtained by CNE.*

99ZL. *The section of the Compliance Guide concerning "Review and Retention" states that GCHQ treats "all operational data" (i.e. including that obtained by CNE) as if it were obtained under RIPA. It sets out GCHQ's arrangements for minimising retention of data in accordance with RIPA safeguards. This is achieved by setting default maximum limits for storage of operational data.*

99ZM. *In addition GCHQ has a separate policy specifically concerning data storage and access. It defines different categories of data, and importantly ascribes specific periods for which different categories of data may be kept, as well as explaining how different categories of CNE data relate to the categories of operational data set out in the Compliance Guide.*

99ZN. *Where CNE analysts identify material as being of use for longer periods than the stipulated limits, it can be retained for longer, subject to justification according to specific criteria.*

99ZO. *Access to data is also subject to strict safeguards, which are set out in the Compliance Guide. CNE content may be accessed by intelligence analysts, but they must first demonstrate that such access is necessary and proportionate by completing a Human Rights Act ("HRA") justification. HRA justifications are recorded and made available for audit. CNE technical data relating to the conduct of CNE operations may only be accessed by a team of trained operators responsible for planning and running such operations.*

99ZP. *GCHQ's policy on storage of and access to data also requires GCHQ analysts who are not in the CNE operational unit to justify access to CNE data on ECHR grounds (particularly*

necessity and proportionality). The justification must be recorded and available for audit.

Handling/disclosure/sharing of data obtained by CNE operations

99ZQ. Pursuant to GCHQ's Compliance Guide, the position is that all operational material is handled, disclosed and shared as though it had been intercepted under a RIPA warrant. The term "operational material" extends to all information obtained via CNE, as well as material obtained as a result of interception under RIPA.

99ZR. The general rules, as set out in the Compliance Guide and the intelligence Sharing and Release Policy which apply to the handling of operational material include, inter alia, a requirement for mandatory training on operational legalities and detailed rules on the disclosure of such material outside GCHQ and the need to ensure that all reports are disseminated only to those who need to see them.

a) Operational data cannot be disclosed outside of GCHQ other than in the form of an intelligence report.

b) Insofar as operational data comprises or contains confidential information (e.g. journalistic material) then any analysis or reporting of such data must comply with the "Communications Containing Confidential Information" section of the Compliance Guide. This requires GCHQ to have greater regard to privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved (e.g. legally privileged material, confidential personal information, confidential journalistic information, communications with UK legislators) GCHQ must accordingly demonstrate to a higher level than normal that retention and dissemination of such information is necessary and proportionate."

77. This is a very full picture of the guidelines under which GCHQ is required to operate, and we are satisfied that they would be adequate, in the context of the

interests of national security, to impose the necessary discipline on GCHQ, and give adequate protection against arbitrary power: further there is, as we have been satisfied, adequate oversight of GCHQ's compliance by the Intelligence Services Commissioner.

78. The nub of the problem arises in two respects, both emphasised by Mr Jaffey:
- i) The impact of the fact that until February 2015, i.e. throughout the period we are addressing, it was not admitted by the Respondent that GCHQ carried out CNE;
 - ii) The impact of the decision of R.E. v UK, in relation to the consideration by the ECtHR.

We will deal with the second submission first.

79. It is important to bear in mind that, as set out in paragraph 74(iii) above, the Court in R.E. v UK was addressing a specific and different question, the matter of adequate protection for LPP communications in respect of covert surveillance. We deal ourselves with LPP as a separate topic in Issue 10 below, and we are not concerned with it in our present considerations. We set out the conclusions of the Court in R.E. v UK in relation to the Revised Code (the Property Code) and Weber (4) to (6), after it has recorded its conclusion that it was satisfied in relation to Weber (1) and (2) (in paragraph 136) and Weber (3) (in paragraph 137):

"138. In contrast, fewer details concerning the procedures to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which recordings may or must be erased or the tapes destroyed are provided in Part II of RIPA and/or the Revised Code. Although material obtained by directed or intrusive surveillance can normally be used in criminal proceedings and law enforcement investigations, paragraph 4.23 of the Revised Code makes it clear that material subject to legal privilege which has been deliberately acquired cannot be so used (see paragraph 75 above). Certain other safeguards are included in Chapter 4 of the Revised Code with regard to the retention and dissemination of material subject to legal privilege (see paragraph 75 above). Paragraph 4.25 of the Revised Code provides that where legally privileged material has been acquired and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during his next inspection. The material should be made available during the inspection if requested. Furthermore, where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, Paragraph 4.26

of the Revised Code states that advice should be sought from a legal advisor before any further dissemination takes place; the retention or dissemination of legally privileged material should be accompanied by a clear warning that it is subject to legal privilege; it should be safeguarded by taking "reasonable steps" to ensure there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings; and finally, any dissemination to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

139. These provisions, although containing some significant safeguards to protect the interests of persons affected by the surveillance of legal consultations, are to be contrasted with the more detailed provisions in Part I of RIPA and the Interception of Communications Code of Practice, which the Court approved in Kennedy (cited above, §§ 42 – 49). In particular, in relation to intercepted material there are provisions in Part I and the Code of Practice limiting the number of persons to whom the material is made available and restricting the extent to which it is disclosed and copied; imposing a broad duty on those involved in interception to keep everything in the intercepted material secret; prohibiting disclosure to persons who do not hold the necessary security clearance and to persons who do not "need to know" about the material; criminalising the disclosure of intercept material with an offence punishable by up to five years' imprisonment; requiring intercepted material to be stored securely; and requiring that intercepted material be securely destroyed as soon as it is no longer required for any of the authorised purposes.

140. Paragraph 9.3 of the Revised Code does provide that each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through directed or intrusive surveillance. In the present case the relevant arrangements are contained in the PSNI Service Procedure on Covert Surveillance of Legal Consultations and the Handling of Legally Privileged Material. The Administrative Court accepted that taking together the 2010 Order, the Revised Code and the PSNI Service Procedure Implementing Code, the arrangements in place for the use, retention and destruction of retained material in the context of legal consultations was compliant with the Article 8 rights of

persons in custody. However, the Service Procedure was only implemented on 22 June 2010. It was therefore not in force during the applicant's detention in May 2010.

141. The Court has noted the statement of the Government in their observations that only one intrusive surveillance order had been granted up till then in the three years since the 2010 Order (introducing the Revised Code) had come into force in April 2010 (see paragraphs 11 and 12 above). Nevertheless, in the absence of the "arrangements" anticipated by the covert surveillance regime, the Court, sharing the concerns of Lord Phillips and Lord Neuberger in the House of Lords in this regard (see paragraphs 36 – 37 above) is not satisfied that the provisions in Part II of RIPA and the Revised Code concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings may or must be erased or the material destroyed provide sufficient safeguards for the protection of the material obtained by covert surveillance.

142. Consequently, the Court considers that, to this extent, during the relevant period of the applicant's detention (4 – 6 May 2010 – see paragraphs 18 – 20 above), the impugned surveillance measures, insofar as they may have been applied to him, did not meet the requirements of Article 8 § 2 of the Convention as elucidated in the Court's case-law."

80. It seems to us entirely clear that they were addressing the adequacy of the Property Code (as compared with the Interception Code) in respect of LPP communications, in relation to which (as discussed in Issue 10) the Government has previously conceded before this Tribunal that the regime established by and for the Intelligence Services was not compliant with the Convention (Belhadi [2015] UKIP TRIB 13_132-8 of 29 April 2015). When the ECtHR addressed, in the cited paragraph 139 above, the benefits of the Interception Code, it is plain to us that they were doing so not in respect of Weber (4) to (6) generally, but in respect of the way in which the Interception Code gave improved safeguards by protecting "the interests of persons affected by the surveillance of legal consultations". The Court did not address specifically, and reach conclusions as to, whether the Property Code was inadequate (other than in respect of LPP) to comply with Weber (4) to (6) in the light of:

- (i) the statutory obligations of and upon GCHQ referred to in paragraph 75 (i) and (ii) above (very much more significant than those imposed upon the Police):

(ii) the provisions of paragraph 9.3 and 9.7 of the Code:

(iii) the *under the waterline arrangements* set out in paragraph 76 above, which we are satisfied were adequately signposted:

(iv) the oversight by the Intelligence Services Commissioner of GCHQ's compliance with their obligations.

Taken together, these are safeguards designed to prevent any arbitrary exercise of the powers to conduct CNE. But none of the safeguards would have been an answer to a system concluded (and now conceded) to have been inadequate in respect of its protection of LPP communications.

81. As to the first submission, as referred to in paragraph 78 (i) above, it is clear that prior to February 2015 there was no admission that property interference by GCHQ (governed by the Property Code) extended to CNE by the use of a s.5 warrant (or *a fortiori* a s.7 authorisation). Nevertheless it was quite clear that at least since 1994 the powers of GCHQ have extended to computer interference (under s.3 of ISA). It was thus apparent in the public domain that there was likely to be interference with computers, 'hacking' being an ever more familiar activity, namely interference with property by GCHQ (and see in particular the 1990 Hansard references in paragraph 18 (iii) above), and that if it occurred it would be covered by the Property Code. Use of it was thus foreseeable, even if the precise form of it and the existence of its use was not admitted.
82. The question is whether we are satisfied that there was, prior to February 2015, adequate protection from arbitrary interference. If there was inadequacy within the Property Code, as compared with the EIC, we do not conclude that the inadequacy was in the circumstances such as to constitute a contravention of Articles 8/10. Compliance with **Weber** (4) to (6) will in our judgment mean the provision, particularly in a national security context, of as much information as can be provided without material risk to national security. In our judgment, not least because of the consequences of a conclusion of unlawfulness simply by virtue of a perceived procedural insufficiency, a conclusion that procedural requirements or the publication of them can be improved (i) does not have the necessary consequence that there has prior thereto been insufficient compliance with **Weber** (4) to (6) and (ii) does not constitute such a material non-compliance as to create a contravention of Article 8. This Tribunal sees it as an important by-product of the exercise of its statutory function to encourage continuing improvement in the procedures adopted by the Intelligence Agencies and their publication (and indeed such improvement took place as a consequence of our Judgments in **Liberty/Privacy No.1**, **Liberty/Privacy No.2** and **Belhadj**), but it does not conclude that it is necessary, every time an inadequacy, particularly an inadequate publication, is identified, to conclude that that renders all previous conduct by the Respondents unlawful. The E I Code is plainly a step forward by the Respondents, which this Tribunal welcomes: taking the Property Code together with the other safeguards which we have set out in paragraph 80 above, we are satisfied that there was prior to that step adequate protection from arbitrary interference.

83. We accordingly resolve Issue 9 in favour of the Respondent. The s.5 regime prior to February 2015 was compliant with the Convention.

Issue 10 Legal and Professional Privilege

84. Issue 10 is: Does the system relating to LPP communications derived from CNE since February 2015 comply with the Convention? Mr Jaffey raised briefly at one stage the question of journalistic sources, but that forms an entirely separate topic, with which this judgment does not deal. The Respondents accepted in Belhadj that since January 2010 the regime for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material has contravened Article 8 ECHR and was accordingly unlawful. This Issue 10 therefore relates only to the period since February 2015 and whether, in relation to LPP, the E I Code has remedied the problem. Mr Jaffey raised only three points by way of continuing criticism, and in the event all of them have become moot so far as any continuing problem is concerned.
85. The first related to GCHQ's definition of legal and professional privilege, which had previously appeared not to include litigation privilege. Mr Jaffey accepts that this has now been made good by the adoption in the E I Code of a definition of privilege analogous to that in the Police Act, which does not exclude litigation privilege.
86. The second criticism related to the fact that the Respondents have said that they were establishing appropriate 'Chinese walls' which would satisfy Mr Jaffey's concerns but did not yet appear to have done so. According to Mr Martin's second statement at paragraph 18, the practice, now described in a document headed "Summary of GCHQ Policy on Handling Material Derived from the Interception of Communications of Individuals Engaged on Legal Proceedings where HMG has an Interest" was still awaiting formal approval. Mr Eadie told us on instructions that the policy had in fact been implemented while still in draft in April 2015, but accepted that nevertheless it had not yet been approved, albeit imminently was to be so. He also referred to paragraph 3.19 of the E I Code, by which the detailed guidance in paragraphs 3.1-3.18, with which Mr Jaffey takes no exception, "*takes precedence over any contrary content of an agency's internal advice or guidance*". Nevertheless we have now been supplied since the hearing with confirmation that this policy was approved, in November 2015.
87. The third problem was that of metadata, which could attract LPP by reference to communications with lawyers, even without their content. There was no dispute between Counsel that metadata might attract LPP. There was no specific mention of metadata in the E I Code, although that of itself would not be a problem. What is a problem is that there is an apparent express exclusion from potentially LPP material of metadata in an internal GCHQ document called "Summary of GCHQ LPP and Sensitive Communications Policy". Because of the lack of mention of metadata in the E I Code, this would not benefit from the 'override' of clause 3.19, and plainly there has been the risk of somebody incorrectly relying upon such guidance. Mr Eadie told us that this guidance would be corrected, and since the hearing a copy of such corrective policy has

been supplied to us, attached as Appendix III: again the underlining denotes gisting.

88. Even without such corrections, Mr Jaffey made clear that none of his criticisms would result in this case in the whole system being unlawful, but it is accepted that there might on the facts (including the facts relating to these Claimants) be a case in which LPP communications have been inappropriately dealt with by virtue of the absence of accurate guidance or policy at the time, and thus amount to a breach of Article 8. There is no need for us to give any specific conclusion in relation to this issue, the discussion of which has once again proved the value of these inter partes proceedings.

Conclusion

89. Our conclusions in relation to the above Issues, where material, are consequently as follows.

(i) Issue 1: An act (CNE) which would be an offence under s.3 of the CMA is made lawful by a s.5 warrant or s.7 authorisation, and the amendment of s.10 CMA was simply confirmatory of that fact.

(ii) Issue 2: An act abroad pursuant to ss.5 or 7 of the ISA which would otherwise be an offence under ss.1 and/or 3 of the CMA would not be unlawful.

(iii) Issue 3: The power under s.5 of ISA to authorise interference with *property* encompasses intangible property.

(iv) Issue 4: A s.5 warrant is lawful if it is as specific as possible in relation to the property to be covered by the warrant, both to enable the Secretary of State to be satisfied as to legality, necessity and proportionality and to assist those executing the warrant, so that the property to be covered is objectively ascertainable, and it need not be defined by reference to named or identified individuals.

(v) Issue 5: There might be circumstances in which an individual claimant might be able to claim a breach of Article 8/10 rights as a result of a s.7 authorisation, but that does not lead to a conclusion that the s.7 regime is non-compliant with Articles 8 or 10.

(vi) Issue 6: A s.5 warrant which accords with the criteria of specification referred to in Issue 4 complies with the safeguards referred to in Weber (1) to (3), and consequently with Articles 8 and 10 in that regard.

(vii) Issue 7: If information were obtained in bulk through the use of CNE, there might be circumstances in which an individual complainant might be able to mount a claim, but in principle CNE is lawful.

(viii) Issue 8: The s.5 regime since February 2015 is compliant with Articles 8/10.

(ix) Issue 9: The s.5 regime prior to February 2015 was compliant with Articles 8/10.

(x) Issue 10: So far as concerns the adequacy of dealing with LPP, the CNE regime has been compliant with the Convention since February 2015.

90. The use of CNE by GCHQ, now avowed, has obviously raised a number of serious questions, which we have done our best to resolve in this Judgment. Plainly it again emphasises the requirement for a balance to be drawn between the urgent need of the Intelligence Agencies to safeguard the public and the protection of an individual's privacy and/or freedom of expression. We are satisfied that with the new E I Code, and whatever the outcome of Parliamentary consideration of the IP Bill, a proper balance is being struck in regard to the matters we have been asked to consider.

APPENDIX I
SCHEDULE
LEGAL ISSUES

Domestic law

1. Prior to the amendments to the Computer Misuse Act 1990 ("CMA 1990") with effect from 3 May 2015, and after those amendments:
 - a. was an act constituting an offence under s.3 CMA 1990 capable of being rendered lawful by a warrant issued under the Regulation of Investigatory Powers Act 2000 ("RIPA 2000") or a warrant or authorisation under the Intelligence Services Act 1994 ("ISA 1994")?
 - b. would the CNE activities of a Crown servant in the course of his employment, if committed in a foreign country or against assets or individuals located in a foreign country, have amounted to an offence under s.3 CMA 1990 as though the activities had been committed in England and against assets or individuals located in England?
2. Does s.5 ISA 1994 permit the issue of a 'class' or 'thematic' warrant, i.e. a warrant authorising certain acts or types of acts in general rather than by reference to specified property or wireless telegraphy?
3. Does the power under s.5 ISA 1994 to authorise interference with "property" encompass physical property only, or does it also extend to intangible legal rights, such as copyright?

ECHR

4. Is the regime which governs Computer Network Exploitation ("the regime") "*in accordance with the law*" under Article 8(2) ECHR / "*prescribed by law*" under Article 10(2) ECHR? In particular:
 - a. Is the regime sufficiently foreseeable?
 - b. Are there sufficient safeguards to protect against arbitrary conduct?
 - c. Is the regime proportionate?
 - d. Was this the case throughout the period commencing 1 August 2009?
5. Specifically:

- a. Should CNE activities be authorised by specific and individual warrants, or is it sufficient that they be authorised by 'class' or 'thematic' warrants or authorisations without reference to a specific individual target?
- b. What records ought to be kept of CNE activity? Is it necessary that records of CNE activity are kept that record the extent of the specific activity and the specific justification for that activity on grounds of necessity and proportionality, identifying and justifying the intrusive conduct taking place?
- c. Have adequate safeguards been in place at all times to prevent the obtaining, storing, analysis or use of legally privileged material and other sensitive confidential documents?
- d. What, if any, is the relevance of the fact that, until February 2015, it was neither confirmed nor denied that the Respondents carried out CNE activities at all?
- e. What, if any, is the relevance of the Covert Surveillance and Property Interference Code, issued in 2002 and updated in 2010 and 2014?
- f. What, if any, is the effect of the publication of a Draft Equipment Interference Code of Practice in February 2015?
- g. What, if any, is the relevance of the Intelligence Services Commissioner's oversight of the use of the powers contained within ISA 1994?
- h. What, if any, is the relevance of the oversight by the Tribunal and the Intelligence and Security Committee of Parliament?

APPENDIX II

Equipment Interference Code of Practice

As approved S.I. 2016 no.38

5. Keeping of records

Centrally retrievable records of warrants

5.1 The following information relating to all section 5 warrants for equipment interference should be centrally retrievable for at least three years:

- All applications made for warrants and for renewals of warrants;
- the date when a warrant is given;
- whether a warrant is approved under urgency procedures;
- where any application is refused, the grounds for refusal as given by the Secretary of State;
- the details of what equipment interference has occurred;
- the result of periodic reviews of the warrants;
- the date of every renewal; and
- the date when any instruction was given by the Secretary of State to cease the equipment interference.

6. Handling of information and safeguards

Overview

- 6.1 This chapter provides further guidance on the processing, retention, disclosure deletion and destruction of any information obtained by the Intelligence Services pursuant to an equipment interference warrant. This information may include communications content and communications data as defined in section 21 of the 2000 Act.
- 6.2 The Intelligence Services must ensure that their actions when handling information obtained by means of equipment interference comply with the legal framework set out in the 1989 and 1994 Acts (including the arrangements in force under these Acts²), the Data Protection Act 1998 and this code, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with this legal framework will ensure that the handling of information obtained by equipment interference continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards against abuse.

² All information obtained by equipment interference must be handled in accordance with arrangements made under section 3(2)(a) of the 1989 Act and sections 3(2)(a) and 4(2)(a) of the 1994 Act (and pursuant to sections 5(2)(c) and 7(3)(c) of the 1994 Act).

Use of information as evidence

- 6.3 Subject to the provisions in chapter 3 of this code, information obtained through equipment interference may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the 1998 Act.

Handling information obtained by equipment interference

- 6.4 Paragraphs 6.6 to 6.11 provide guidance as to the safeguards which must be applied by the Intelligence Services to the processing, retention, disclosure and destruction of all information obtained by equipment interference. Each of the Intelligence Services must ensure that there are internal arrangements in force, approved by the Secretary of State, for securing that these requirements are satisfied in relation to all information obtained by equipment interference.
- 6.5 These arrangements should be made available to the Intelligence Services Commissioner. The arrangements must ensure that the disclosure, copying and retention of information obtained by means of an equipment interference warrant is limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes set out in section 2(2)(a) of the 1989 Act and sections 2(2)(a) and 4(2)(a) of the 1994 Act. Breaches of these handling arrangements must be reported to the Intelligence Services Commissioner as agreed with him.

Dissemination of information

- 6.6 The number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. This obligation applies equally to disclosure to additional persons within an Intelligence Service, and to disclosure outside the service. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: information obtained by equipment interference must not be disclosed to any person unless that person's duties are such that he needs to know about the information to carry out those duties. In the same way only so much of the information may be disclosed as the recipient needs; for example if a summary of the information will suffice, no more than that should be disclosed.
- 6.7 The obligations apply not just to the Intelligence Service that obtained the information, but also to anyone to whom the information is subsequently disclosed. In some cases this may be achieved by requiring the latter to obtain the originator's permission before disclosing the information further. In others, explicit safeguards may be applied to secondary recipients.

Copying

- 6.8 Information obtained by equipment interference may only be copied to the extent necessary for the proper discharge of the Intelligence Services' functions or for the additional limited purposes described in paragraph 6.5. Copies include not only direct copies of the whole of the information, but also extracts and summaries which identify

themselves as the product of an equipment interference operation. The restrictions must be implemented by recording the making, distribution and destruction of any such copies, extracts and summaries that identify themselves as the product of an equipment interference operation.

Storage

- 6.9 Information obtained by equipment interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance. This requirement to store such information securely applies to all those who are responsible for the handling of the information.

Destruction

- 6.10 Communications content, communications data and other information obtained by equipment interference, and all copies, extracts and summaries thereof, must be marked for deletion and securely destroyed as soon as they are no longer needed for the functions or purposes set out in paragraph 6.5. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.

Personnel security

- 6.11 In accordance with the need-to-know principle, each of the Intelligence Services must ensure that information obtained by equipment interference is only disclosed to persons as necessary for the proper performance of the Intelligence Services' statutory functions. Persons viewing such product will usually require the relevant level of security clearance. Where it is necessary for an officer to disclose information outside the service, it is that officer's responsibility to ensure that the recipient has the necessary level of clearance.

Appendix III

Reporting LLP

Legally privileged communications

The GCHQ Compliance Guide explains that the RIPA Interception of Communications Code of Practice stipulates that greater regard should be had for privacy issues where the subject of the interception might reasonably assume a high degree of privacy or where confidential information is involved. This means that there are certain categories of communication where a particular high threshold of proportionality must be applied to the release of the content, because the content of the communication would ordinarily be considered confidential (in the common sense of the word) or otherwise privileged. These categories are:

- Legally privileged communications;
- Personal information held in confidence relating to physical or mental health;
- Personal information held in confidence relating to spiritual counselling;
- Confidential journalistic material;
- Confidential constituent information

Legal Professional Privilege (LPP) broadly falls into two categories.

-legal advice privilege which attaches to communications between a professional legal adviser, acting as such, and their client where the communications are made confidentially for the purpose of seeking or providing legal advice.

-litigation privilege which attaches to communications between the client and his legal adviser or agent, or between one of them and a third party, if such communications come into existence for the sole or dominant purpose of either seeking or providing legal advice with regard to litigation or collecting evidence in respect of litigation. This second category is wider than the first since it is possible for litigation privilege to attach to communications other than those directly between a lawyer and their client, *i.e.* privilege can attach to communications between a lawyer and a third party where such communications are in connection with legal proceedings.

The concept of LPP applies to:

- The content of communications that fall into one of the categories above, and
- Exceptionally, some communications data (*i.e.* 'events' or the fact of a communication),

The purpose of LPP is to ensure that individuals are able to consult a lawyer in confidence without fear that what passes between them will later be used against them in court and it is therefore fundamental to the right to a fair trial and the rule of law. Intelligence material subject to LPP cannot be released to a customer who may be a party to any legal case to which the material relates, because this would give that customer an unfair litigation advantage (it being a basic principle that litigants cannot be required to reveal privileged material to either their opponents or the

court in a given piece of litigation). However, communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably) are unlikely to be protected by LPP. For more details contact the Disclosure Policy team.

The judgment as to whether it is necessary and proportionate to include information subject to LPP in the release of intelligence material by GCHQ must take account of the particular sensitivity of such information and any associated risks. It is likely that any release of material protected by LPP that is deemed both necessary [and] proportionate will be to a more limited readership limited and possibly more highly classified than would otherwise be the case. The judgment of necessity and proportionality in these cases is reserved to Mission Policy, and all reporting containing anything that you believe may be covered by LPP must be submitted for checking. For the sake of simplicity, in order to ensure that all intelligence material containing potentially LPP information is submitted and assessed, reports featuring the following types of intelligence must be submitted for checking before issue:

- Content and/or communications data ('events') relating to (including instances where a target has been in contact with) lawyers, legal advisers, solicitors, attorneys, or any other member of the legal profession, or content that includes legal advice, regardless of the profession of the communicant.

The sensitivity of reporting LPP information is not mitigated by disguising or removing the identity or occupation of the communicant. But neither is there a 'ban' on identifying or reporting such material – it may well be necessary and proportionate to report such information to certain circumstances. The checking process is designed to determine this. If Mission Policy considers it proportionate in a particular case to release intelligence based on communications that attract legal privilege, the reporter will be instructed to apply the following rubric to the report:

This report contains material that may be subject to legal professional privilege, and onward dissemination/Action On is not to be taken without reverting to GCHQ.

Mark Scott
Bhatt Murphy
27 Hoxton Square
London N1 6NN

Our ref: IPT 14/85/CH

IPT 14/120-126/CH

Date: 09 March 2016

Dear Sirs

I write in connection with your clients' applications to the Investigatory Powers Tribunal received 4 July 2014.

The Investigatory Powers Tribunal has carefully considered your clients' complaints and Human Rights Act claims in the light of all relevant evidence and in accordance with its normal procedures. The Tribunal has asked me to inform you that no determination has been made in your favour either on your complaints or your Human Rights Act claims.

Under section 68 (4) of the Act when not making a determination in favour of an applicant, the Tribunal is only permitted to inform such complainants that no determination has been made in their favour.

For the avoidance of doubt the Tribunal has not been required to consider, and has not considered, the matters left open in paragraphs 53 and 63 of the Privacy/Greennet Judgment.

Yours sincerely



Mr S Wilkins
Tribunal Secretary

○

○