IN THE INVESTIGATORY POWERS TRIBUNAL

BETWEEN:

PRIVACY INTERNATIONAL

Claimant

-and-

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

Defendants

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*".[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 Privacy International

19. In order to pursue this complaint, Privacy International need not show that it ~~is~~ 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*

[10] 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*"~~is~~ 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).

<u>*Domestic legal regime governing the relevant conduct*</u>

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.

Computer Misuse Act 1990

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~~s.10 CMA 1990 provide~~d~~s 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~~are~~ *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 concerned[11]; 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. Prior 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.

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 ~~by the Secretary of State is lawful~~; and

~~a.~~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

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.

---

both Houses of Parliament. The Claimant has lodged representations on the draft Code, a copy of 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.

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