IN THE EUROPEAN COURT OF HUMAN RIGHTS **Application No. 46259/16**

B E T W E E N:

(1) PRIVACY INTERNATIONAL

(2) GREENNET LIMITED

(3) CHAOS COMPUTER CLUB E.V.

(4) MEDIA JUMPSTART INC.

(5) RISEUP NETWORKS INC.

(6) KOREAN PROGRESSIVE NETWORK JINBONET

Applicants

-v-

THE UNITED KINGDOM

Respondent

APPLICANTS' OBSERVATIONS AND REPLY TO OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY

A. Significance of the application

1. The application concerns the regime that was in force in the UK before 31 May 2018, governing the use of Computer and Network Exploitation ("CNE", usually known as 'computer hacking') by the UK intelligence services. This application focuses mainly (but not exclusively)[1] on CNE on devices and networks outside the British Islands[2]. Although the devices interfered with are mostly outside of the British Islands, the data taken is transferred back to the UK, where it is analysed and the key interferences with privacy occur, as with bulk interception operations.

2. Specifically, the Applicants challenge the compatibility of section 7 of the Intelligence Services Act 1994 ("ISA") with Articles 8, 10 and 13 of the Convention. Section 7 ISA permits the interception or obtaining, processing, retention, examination, alteration or modification of private – and in certain cases extremely intimate or sensitive – information belonging or relating to very large numbers of people. In some cases, the whole population of a country or region could have their data taken in bulk. Section 7 also permits serious invasions of journalistic and watchdog organisations' materials and lawyer–client communications.

3. As a form of surveillance, "*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*".[3] The sophistication of this surveillance activity varies. CNE operations differ in their scope and complexity. At the simplest end, they may involve "*using the login credentials of a target to gain access to the data held on*" a device. More complex CNE may involve "*taking advantage of weaknesses in software*" (vulnerabilities).[4] The exploitation of these weaknesses allows for the installation of another piece of software (implant), which "*will typically explore the target computer, sending back information over the Internet to its controller*" or

[1] Section 7 ISA 1994 is primarily concerned with acts done "*outside the British Islands*". However, subsections (10)-(12) make provision for certain acts to be treated as if they were done outside the British Islands even if they were not: for example, if the act relates to property which was wrongly believed to be outside the British Islands, or if the act is done within 5 working days of discovering that that belief was incorrect.
[2] The United Kingdom of Great Britain and Northern Ireland, the Channel Islands and the Isle of Man.
[3] Witness Statement of Ciaran Martin, 16 November 2015, para 21 (lodged with the Court in the List of Accompanying Documents in the original Application) ("Martin Witness Statement").
[4] Ibid, paras 22-23.

"*monitor the activity of the user of the target device*" or even "*take control*" of the device.[5] The equipment that CNE can interfere with "*may include, but is not limited to, "computers, servers, routers, laptops, mobile phones and other devices*".[6] The most complex and wide-ranging forms of CNE may interfere with entire portions of the internet, servers, routers or entirely categories of device, or all users of a particular piece of hardware or software (e.g. by interfering with hardware at the point of production, or by altering software used by a large number of users).

4. CNE is thus a powerful and flexible technique, which can involve greater risks to the privacy and the security of the community than any other form of surveillance, especially when involves the manipulation of devices to acquire vast amounts of personal data in bulk.[7] This is because unlike traditional targeted or bulk interception techniques, CNE enables the collection and analysis of highly personal data which individuals might have never wished to communicate over a computer network to another, such as private notes, diaries, photographs and other biometric data, credit card data, research material, information covered by journalistic or legal profession privilege.[8] There is an important difference between private information that we choose to store only on our computers and information that we choose to communicate to others. As the Government admit in their Observations (§9), CNE enables the SIAs to obtain "*communications and data of individuals"* which *"may not have been communicated*". In respect of this data individuals hold a greatly increased expectation of privacy as compared to data transmitted over a public communications network.

5. The greater intrusiveness of these new techniques has not been accompanied by a commensurate increase in the safeguards that accompany such intrusive surveillance technologies. In fact, what the Government now describes as "*a critical tool in investigations into the full range of threats to the UK*" (Observations, §8) was until recently an entirely undisclosed and unacknowledged capability with no published safeguards or parameters of any kind, kept entirely secret until it was belatedly avowed in 2015 in response to a challenge brought by the Applicants. Even once avowed, CNE

[5] Ibid, paras 23-25.
[6] Independent Reviewer of Terrorism Legislation, A Question of Trust: Report of the investigatory powers review (2015) (lodged with the Court in the List of Accompanying Documents in the original Application), para 6.25., and the sources referred to therein, ("A Question of Trust").
[7] Ibid, para 10.40.
[8] Witness Statement of Eric King, 5 October 2015, paras 26-28 and the sources referred to therein (lodged with the Court in the List of Accompanying Documents in the original Application) ("King Witness Statement").

was regulated under a minimal and inadequate scheme under which unprecedentedly large scale intrusions could occur, with similar problems to the arrangements for interception that this Court found to be unlawful in *Malone v. UK* (App. No. 86/91/79, 2 August 1984), a case decided 35 years ago.

B. Unprecedented Privacy Threats

6. The use of CNE to obtain confidential material held on a device or network itself involves a greater intrusion than the interception of communications in the course of their transmission. But it is only one of a range of novel forms of surveillance which CNE permits governments to conduct. For example, CNE may be used to activate sensors on a device, such as by covertly turning on a device's microphone, camera, or GPS-based location technology.[9] Through CNE, a government can also capture continuous screenshots of the hacked device or see anything input into and output from that device, including login details and passwords, internet browsing histories etc.[10] There is no theoretical limit to the range of devices to which CNE may be directed, as long as it is possible to gain access remotely; such activity could readily extend to digitally enabled home and personal devices, or body-worn or embedded devices such as health sensors or smart watches.

7. The degree of intrusiveness caused by this access to modern devices has been recognised by other courts. For example, in *Riley v. California*, 573 US _ (2014), in the Supreme Court of the United States, Chief Justice Roberts noted the exceptional intrusiveness of gaining access to a modern mobile telephone:

> "*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 [...] The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet*." (p. 18)

8. In *Ivaschenko v. Russia* (App. No. 61064/10, 13 February 2018), this Court affirmed:

[9] A Question of Trust, Annex 7, paras 15-18, and the sources referred to therein.
[10] King Witness Statement, paras 19-25 and the sources referred to therein.

"*it is usual for an electronic device to contain various types of electronic files (text, photographs, videos and others) and that the contents may vary even within the same type of file.*" (§83).

9. CNE also permits governments to edit, delete, modify, or falsify data on a device. It can also be used to recover data that has been deleted, send fake communications or data from the device, or add or edit code to add new capabilities or alter existing ones and erase any trace of the intrusion.[11] In a world where information about us is increasingly expressed as data, minute changes to that data – a password, GPS coordinates, a document – can have radical effects. CNE is therefore not simply a passive technique of interception. It can be used to substantively interfere with property and reputation.

10. The privacy intrusions of CNE are amplified should a government interfere with communications networks and their underlying infrastructure. By hacking a network provider, for instance, a government might gain access not only to the provider's system, but also (through the data stored there) to the systems of all its users.[12] Governments may also interfere with different types of networks and their infrastructure, such as those connecting banks.[13] CNE directed at networks could be for the purpose of conducting surveillance against specific individuals, groups or countries, or across numerous jurisdictions.[14] CNE directed at a bank could lead to the compromise of all of its customers' data. Or CNE directed at the manufacturer of a mobile telephone or SIM card could lead to the compromise of the data of everyone who uses a particular kind of device.

C. Novel security risks

11. Computer systems, especially computer software programs, are complex. Inevitably, they contain vulnerabilities. People are also complex and their interactions with systems also give rise to vulnerabilities.[15]

[11] King Witness Statement, paras 32-33.
[12] Ibid, paras 34-40.
[13] Ibid, para 132.
[14] Ibid, paras 34ff.
[15] Expert Report of Professor Ross Anderson (30 September 2015), para 23 (lodged with the Court in the List of Accompanying Documents in the original Application) ("Anderson Expert Report").

12. CNE operations rely to a great extent on the exploitation of system vulnerabilities, such as 0-day vulnerabilities, which are security flaws in software which are unknown to the vendor. When researchers and others discover vulnerabilities, they usually report the flaw to the company responsible for the security of the affected software so that the flaw gets fixed before third parties discover it first and exploit it unlawfully.[16]

13. In the surveillance context, the government identifies vulnerabilities, not to secure systems through testing and coordinated disclosure, but to exploit them to facilitate a surveillance objective.[17] This activity may not only undermine the security of the target system but also of other systems.[18] It also raises significant concerns, as the intervenors submit, regarding whether the use of CNE prevents Council of Europe member States from complying with their positive obligations, under the Convention, to guarantee and protect the confidentiality, integrity and security of systems and personal data.

14. Therefore, this application raises novel and important issues of law and principle: it is the first time this Court has been called upon to address directly the question of whether CNE on the scale now taking place[19] should be permitted and the minimum safeguards that are needed to meet the standards required by the Convention, taking into account its unprecedentedly intrusive nature in an age of digital communication.

15. For that reason, the Court is invited to consider the section 7 CNE Regime with care. On examination, it neither meets the requirements for being "*in accordance with law*" nor is it necessary or proportionate.

16. First, the section 7 CNE Regime was and remains opaque. It was not until Edward Snowden disclosed the existence and extent of the UK Government's bulk CNE operations – in particular, a number of programmes that involved implanting malware in bulk[20] – that the public first became aware of these intrusive capabilities. However, even then the Government did not admit that it carried out CNE until, over a year later, it

[16] King Witness Statement, paras 73-80.
[17] Anderson Expert Report, paras 37-41.
[18] Anderson Expert Report, paras 74-77. See also ISC Report, p. 69 DD.
[19] "*CNE operations have been authorised by senior Ministers for many years since the 1994 Act, but its importance relative to the GCHQ's overall capabilities has been increasing significantly in recent years and is likely to increase further*", Martin Witness Statement, para 20; "*During 2013 a significant number … of GCHQ's intelligence reports contained information that derived from IT Operations against a target's computer or network*", Intelligence and Security Committee of Parliament, Privacy and Security (12 March 2015) (lodged with the Court in the List of Accompanying Documents in the original Application) ("ISC Report") p. 67.
[20] A Question of Trust, Annex 7, paras 15-18.

published a Draft Equipment Interference Code in the course of defending the IPT proceedings brought by the Applicants. Further, the Equipment Interference Code only has statutory force in relation to the exercise of the power under section 5 ISA 1994, a more limited power which is exercisable within the British Islands: it is of no legal effect in relation to the exercise of the (already looser and more expansive) power under section 7, and is said to be treated as applicable to that power only "*as a matter of policy*".[21]

17. Section 7 ISA 1994, the only statutory provision regulating CNE conducted outside the British Islands, is also known as the "James Bond" clause, due to the extremely vague and broad powers it confers to commit criminal offences and torts. In other words, the only legal regime regulating CNE outside the UK is a vague *"power for the Foreign Secretary to authorise GCHQ or MI6 to carry out acts outside the British Islands that might otherwise be criminal offences or give rise to civil liability*".[22]

18. Second, the section 7 CNE Regime fails to meet the minimum safeguards for surveillance operations identified in *Weber and Saravia v Germany* (App. No. 54934/00, 29 June 2006). Those safeguards should be applied to CNE, which, if anything, is likely to be much more intrusive than mere intercept. Furthermore, in its recent case law, the Court has made clear that significant technological developments in electronic communications and covert surveillance capabilities should be matched by commensurate developments in the minimum legal safeguards applicable to a state's use of covert surveillance powers. As the Court declared in *Szabó and Vissy v. Hungary* (App. No. 37138/14, 12 January 2016), *"[t]he guarantees required by the extant case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices*." (§70).

19. Thirdly, in light of the seriousness of the interference caused by CNE, the court's existing minimum safeguards ought to be enhanced to require: (1) individual reasonable suspicion regarding the target of a CNE operation; (2) prior independent authorisation of a CNE operation; and (3) subsequent notification of the CNE operation where notification would be compatible with the public interest.

20. Fourthly, the Applicants adopt and agree with the Submissions put forward by some of the Third Party Intervenors that the section 7 CNE Regime poses serious additional

[21] Judgment of Investigatory Powers Tribunal on Preliminary Issues (12 February 2016)) (lodged with the Court in the List of Accompanying Documents in the original Application) ("IPT Judgment"), para 49.
[22] A Question of Trust, para 6.27.

threats to the security of individuals' personal data, devices, IT systems and networks because acts of CNE can have the secondary consequence of further exposing individuals and their devices to nefarious exploitation by third parties, for instance by making use of vulnerabilities that are introduced.[23] By deploying CNE without taking adequate steps to guard against these security concerns, the Government fails to meet their positive obligation to effectively guarantee the protection enshrined in Article 8 of the Convention.

21. For all of these reasons, interferences with privacy and freedom of expression authorised under the s8(4) Regime are not in accordance with law.

22. Bulk CNE is also neither necessary nor proportionate. The Government maintains that, "*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*" (Observations, §8). The Applicants agree that the UK faces serious security risks and that properly targeted and authorised surveillance measures can assist in the prevention and prosecution of serious crimes. The Applicants further recall the Government's similar claim in *S. and Marper v. United Kingdom* (App. Nos. 3562/04 and 30566/04, 4 December 2008) that DNA material taken from persons who had not been convicted of any criminal offence was "*of inestimable value in the fight against crime and terrorism and the detection of the guilty*" (§91). In that case, the Grand Chamber unanimously concluded that despite the existence of evidence showing the usefulness of a DNA database, the "*blanket and indiscriminate" nature of the Government's retention of personal data "fail[ed] to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard*" (§125). Usefulness is not the same thing as proportionality. Many things that an intelligence service would find useful, even extremely valuable, are not permissible in a democratic society.

23. Here, the blanket and indiscriminate nature of the section 7 CNE Regime fails to strike a fair balance between public and private interests and similarly oversteps any acceptable margin of appreciation. As the Grand Chamber held in *Klass v. Germany* (App. No.

[23] Intervention by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (16 September 2019); Written Comments of Third Party Intervener Mozilla (13 September 2019).

5029/71, 6 September 1978): "*The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate*" (§49).

II. FACTS

A. The CNE Regime under section 7 of the Intelligence Services Act 1994

24. Section 7 of the Intelligence Services Act 1994 ("ISA") allows the Secretary of State to authorise a person to undertake (and thereby to exempt that person from criminal or civil liability for) an act outside the British Islands in relation to which they would be liable if it were done in the United Kingdom.

25. The 2015 ISC Report states at (§236):

> "*In recent years, many people have expressed suspicion as to the true nature of Section 7 of ISA, with some referring to it as the 'James Bond clause' and suggesting that it might allow serious crimes to be committed.*"

26. These legitimate concerns, stemming from the extremely vague and broad powers section 7 ISA confers, are further articulated in the 2015 Report of the Independent Reviewer of Terrorism Legislation:

> "*ISA 1994 s7 (which has been referred to as the "James Bond clause") provides a power for the Foreign Secretary to authorise GCHQ or MI6 to carry out acts outside the British Islands that might otherwise be criminal offences or give rise to civil liability. GCHQ had five s7 class-based authorisations in 2014, removing liability for activities including those associated with certain types of intelligence gathering and interference with computers, mobile phones and other types of electronic equipment. MI6 had eight class-based authorisations, removing liability for activities such as the identification and use of CHIS, directed surveillance and interference with and receipt of property and*

documents, and may seek further ministerial authorisations in respect of specific operations." [24]

B. CNE as a surveillance technique

27. CNE is a powerful and highly intrusive surveillance technique.[25] When deployed against an individual's device, CNE can thus achieve results that are at least as intrusive as if the targeted individuals were to have their house bugged, their home searched, their communications intercepted and a tracking device fitted to their person.[26] As Eric King put it in his Witness Statement before the IPT:

> "*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*." (§11)

28. The IPT's Judgment of 12 February 2016 states at (§5) that GCHQ admits that:

    28.1 GCHQ undertakes CNE operations both within the UK and overseas.

    28.2 GCHQ undertakes both *"persistent"* CNE operations (where an implant *"resides"* on a computer for an extended period) and *"non-persistent"* operations.

    28.3 The Agencies' CNE activities include operations against specific devices, computer networks and other targets.

    28.4 GCHQ has obtained warrants to authorise CNE under both section 5 and section 7 ISA 1994.

    28.5 GCHQ had five class authorisations under section 7 in 2014.

    28.6 In 2013, about 20% of GCHQ's intelligence reports contained information derived from CNE.

[24] A Question of Trust, para 6.27.
[25] Martin Witness Statement, paras 28ff.
[26] King Witness Statement, paras 9-10.

29. The key features of CNE are as follows.

30. 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,[27] for instance:

    30.1 photos or videos stored on the device;

    30.2 documents;

    30.3 address book;

    30.4 location, age, gender, marital status, finances, ethnicity, sexual orientation, education and family; and

    30.5 information collected through activation of the device's microphone or camera without the user's consent.[28]

31. The agencies have the technological capability to acquire all such information from a user's device. David Anderson QC in his report *A Question of Trust* refers to documents disclosed by Edward Snowden which explain 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.*"[29]

32. Secondly, CNE involves an active intrusion into a device or network. CNE techniques are not limited to the acquisition of information; they can potentially be used to amend, add, modify or delete information, or to instruct the device to act or respond differently to commands.[30]

[27] Government Observations, para 9.
[28] King Witness Statement, para 10.
[29] A Question of Trust, Annex 7, paras 15-18.
[30] IPT Judgment, para 9; Martin Witness Statement, para 46.

33. Thirdly, 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.[31] For example, it appears that GCHQ 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*".[32] An operation of that kind would result in the encryption included in every mobile phone using a SIM card made by a leading manufacturer being deliberately compromised. The scale and reach of such an operation would be exceptionally wide and the effects broad and long-lasting.

34. Other examples include a CNE operation giving the relevant agency access to "*almost any user of the Internet*" in a targeted country[33] and systems designed for "*industrial scale exploitation*", appropriating the processing power of the target's computers to carry out searches and bulk analysis work.[34]

35. Fourthly, CNE may leave users vulnerable to further damage. As Professor Ross Anderson explained in his Expert Report to the IPT (§§49-77):

    35.1 Malware installed on a device can be used by third parties, with similarly intrusive effects or worse.

    35.2 The process necessary to install the malware without alerting the user or his security software may create or preserve security vulnerabilities that could be exploited by third parties in other ways.

    35.3 If the CNE takes place on a large scale – for instance in relation to network infrastructure, software, or common security protocols, by introducing a vulnerability at source with a view to facilitating future CNE operations – it weakens security for all users, increasing the risk of exploitation by a third party.

C. The Investigatory Powers Tribunal

36. In May 2014, the Applicants brought proceedings in the IPT challenging Section 7 ISA 1994, the statutory power relied upon as justifying CNE outside the British Islands, as

[31] IPT Judgment, para 9.
[32] King Witness Statement, para 55.
[33] King Witness Statement, para 40.
[34] King Witness Statement, paras 42 and 138.

contrary to domestic law and the European Convention on Human Rights. The Applicants contended that CNE constituted a serious interference with their Convention rights and that this interference was neither in accordance with the law (Article 8)/prescribed by law (Article 10) nor necessary in a democratic society.

37. At that stage, there was no public acknowledgement that CNE was even being carried out, let alone any published information about any safeguards governing its use. In February 2015, on the same day that the Respondents served their response to the complaint in the IPT, the UK Government published a Draft Equipment Interference Code which admitted the use of CNE for the first time ("the First Draft EI Code"). A Second Draft was published during the course of the proceedings, and the Equipment Interference Code was promulgated under s.71 RIPA 2000 in January 2016.

38. However, the statutory provision which gives that Code legal force (s.71 RIPA 2000) applies only to the exercise of the power under section 5 ISA. There is no equivalent power to issue a Code of Practice in respect of the exercise of the power under section 7 ISA. The Draft EI Codes, and the version promulgated under s.71 in January 2016, contain provisions relating to the exercise of that power, but they expressly note the absence of statutory underpinning for those provisions and make clear that the provisions are complied with "*as a matter of policy*".

39. The IPT held a hearing which lasted for three days during which it heard argument from the parties' legal representatives. It gave judgment on 12 February 2016.[35]

40. Examining first the domestic legal regime, the IPT drew a distinction between the two regimes governing CNE operations carried out by the UK security and intelligence services ("UKSIS"), namely the section 5 ISA CNE Regime and the Section 7 ISA CNE Regime. While the former is based on section 5 ISA which is domestic focused and only permits property interference or interference with wireless telegraphy,[36] the latter is based on section 7 ISA which is limited to activities outside the British Islands[37] and can cover any potentially criminal activity.[38]

[35] Ibid.
[36] Section 5 ISA 1994; A Question of Trust, para 6.26.
[37] Index of Open Exhibits to Re-re-amended Open Response, Exhibit 4 (Extract from current Advanced Training for Active Operations).
[38] Index of Open Exhibits to Re-re-amended Open Response, Exhibit 1 (Compliance Guide –Authorisations).

41. The IPT frankly explained the lack of statutory safeguards for the use of the s. 7 ISA power. It held (§49) that it "*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*".

42. The IPT concluded that acts of CNE which would be unlawful under the Computer Misuse Act 1990 ("CMA"), were rendered lawful where a warrant or authorisation to conduct Equipment Interference had been obtained under sections 5 or 7 of the ISA, respectively.

43. Having considered domestic lawfulness, the IPT turned expressly to the Convention arguments and set out its conclusions concerning section 7 ISA authorisations (in relation to acts done outside the British Islands) in paragraphs 53 and 63 of its decision.

44. It considered first the question of jurisdiction and whether CNE undertaken outside the United Kingdom would come within the scope of the Convention. It contrasted the scope of section 7 (which was concerned primarily with acts "*outside the British Islands*") with Contracting States' obligations to secure to everyone "*within their jurisdiction*" the rights and freedoms set out in the Convention.

45. At (§50), it noted:

> "*It was, in the event, common ground that, subject to [counsel for the Applicants] 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.*"

46. At (§53), the IPT went on to say:

"*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.*"

47. The IPT then turned to examine the complaint about "*bulk CNE [Equipment Interference]"*, under section 7. So far as it concerned the section 7 regime the IPT concluded with reference to what was then future legislation:

> *"62. Both aspects of [the Applicants'] complaints appear to have been taken up in the IP Bill [new legislation then before Parliament]. 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."*

48. The IPT concluded:

> "*89. […]*

(i) Issue 1 [S.10 of the CMA]: 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 [Territorial jurisdiction in respect of ss.5/7]: 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. […]

(v) Issue 5 [Scope of the Convention]: 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. […]

(vii) Issue 7 [Bulk CNE]: 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. […]

90. The use of CNE [Equipment Interference] 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 [Equipment Interference] Code and whatever the outcome of the Parliamentary consideration of the IP Bill, a proper balance is being struck in regards to the matters we have been asked to consider (emphasis added)."

49. On 9 March 2016 the IPT sent the applicants a formal "*no determination letter*" which read as follows:

"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. […]

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."

III. CNE UNDER SECTION 7 ISA BREACHES THE CONVENTION

A. CNE is extremely and unprecedentedly intrusive

50. For the reasons set out above, CNE as permitted under section 7 ISA constitutes a very serious interference with privacy. It allows for the bulk or large-scale processing of personal data, including data which individuals might have never intended to communicate over a network (or possibly at all) and for which they therefore hold a high expectation of privacy.

51. As such, the interference with Convention rights created by the legal regime for CNE must be "*in accordance with law*" and "*necessary in a democratic society*".

52. These requirements exist because secret surveillance must be subject to a clear and (so far as possible) public legal regime, with adequate safeguards to protect liberty and prevent arbitrary use. The UK Independent Reviewer of Terrorism Legislation has explained the importance of both safeguards and firm limits on the use of mass surveillance technology, and of bearing in mind that not everything that is useful to a secret intelligence service is permissible in a democratic society:

"The capabilities of the state are subject to technical or cost-based limits. But 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 […]

Some might find comfort in a world in which our every interaction and movement could be recorded, viewed in real-time and indefinitely retained for possible future use by the authorities. Crime-fighting, security, safety or public

health justifications are never hard to find... The impact of such powers on the innocent could be mitigated by the usual apparatus of safeguards, regulators and Codes of Practice. But a country constructed on such a basis would surely be intolerable to many of its inhabitants. A state that enjoyed all those powers would be truly totalitarian, even if the authorities had the best interests of its people at heart. There would be practical risks: not least, maintaining the security of such vast quantities of data. But the crucial objection is of principle." [39]

B. CNE as permitted under section 7 ISA is not "in accordance with the law"

(i) The CNE Regime was neither foreseeable nor accessible

Prior to the publication of the first Draft EI Code

53. In *Zakharov*, the Grand Chamber "*note[d] from its well established case-law that the wording 'in accordance with law' requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law*". It elaborated that "*[t]he law must thus meet quality requirements; it must be accessible to the person concerned and foreseeable as to its effects*". (§228).

54. In addition, the Court in *Zakharov* emphasised that "*the reference to 'foreseeability' in the context of interception of communications cannot be the same as in many other fields*." Given that "*where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident*", the Court stated that it is "*therefore essential to have clear, detailed rules*" regulating interception "*especially as the technology available for its use is becoming increasingly more sophisticated*." Thus, "*[t]he domestic law must be sufficiently clear 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*". (§229).

55. The Applicants also note that, in *Khan v. UK*, the Court held, first, that the non-statutory Home Office Guidelines on the use of equipment in police surveillance operations "*at*

[39] A Question of Trust, paras 13.18-13.21.

the relevant time *were neither legally binding nor were they directly publicly accessible*" (*Malone v. UK*, §27).

56. The position under the CNE regime prior to publication of the EI Code was therefore even worse than the pre-IOCA 1985 days of intercept considered by the ECtHR in Malone. CNE was being used under a general statutory power in s. 7 ISA (which did not even refer to CNE – it simply permitted the Secretary of State to authorise acts which would otherwise be unlawful). Nothing was known in public about the government's use of CNE. Even the fact CNE was carried out was an official secret. At least in *Malone* the fact that the government used interception capabilities was openly known. The position prior to the first EI Code is also worse than in *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.

57. The failing is not simply technical. As David Anderson QC puts it (§13.31):

> "*Obscure laws –and there are few more impenetrable than RIPA and its satellites [of which ISA is one] – 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.[…] section 7 ISA 1994 is:*
>
> *(a)... so baldly stated as to tell the citizen little about how they are liable to be used*."

58. Before the publication of the First Draft EI Code, none of the publicly available legislative instruments contained any reference to the term CNE or hacking or even equipment interference. Further, until partway through the IPT proceedings, GCHQ refused even to confirm or deny whether it had CNE capabilities, or had ever used them. The first public disclosure of these highly intrusive capabilities came with the revelations of former NSA contractor Edward Snowden.[40] As the Independent Reviewer of Terrorism Legislation said in his 2015 Report:

> "*Though EI (then known as CNE) was only avowed in February 2015, the Snowden documents had suggested that it was being practised some years*

[40] A Question of Trust, para 1.8.

before that date, and many of the criticisms are based upon readings of those documents." [41]

59. However, it was only in February 2015, during the domestic proceedings that underly this application, that the UK government produced its first draft EI code. This was the first time that an instrument with any reference to CNE capabilities was made public by the UK authorities.

60. The publication of the draft Codes makes the unlawfulness of the prior position clear. In February 2015 the Government considered it possible to avow the existence of CNE activities and to publish information about how the relevant powers were exercised. There was no suggestion at that stage that the publication of that information created an unacceptable risk of harm to national security. Nor was there any suggestion that any recent developments immediately prior to February 2015 had made it possible to publish information that could not have been published before. It follows that there was no compelling reason why the disclosures made in February 2015 could not have been made sooner. The regime as it existed prior to those disclosures, where the existence of the capability was not acknowledged even though (by the above logic) there was no good reason why it could not have been, was therefore unlawful.

61. The Tribunal appeared to accept that logic, which is clear and inescapable. It nevertheless declined to make a finding of unlawfulness on the grounds that to do so would disincentivise future steps by the intelligence services to improve their arrangements. It cannot be relevant to the application of the legal requirements of Article 8 that the state whose conduct is challenged might react poorly to a finding of infringement. At most, the steps taken by a state after a period of infringement are capable of being relevant to the question of what relief it would be appropriate to order. They cannot affect the question whether the conduct prior to the taking of those steps amounted to an infringement.

62. Consequently, the Applicants invite the Court to make a finding that the section 7 ISA regime insofar as it was used to authorise CNE prior to the promulgation of the EI Code

[41] A Question of Trust, para 2.67.

in January 2016, or alternatively the publication of the first draft EI code in February 2015, was not "in accordance with law" and that it violated the Convention.

(ii) After to the publication of the first Draft EI Code

63. Even after the publication of the Draft EI Code and its adoption, the s. 7 regime still does not meet the accessibility and foreseeability requirements of the Convention.

64. The level of precision required for domestic laws to meet the standard of foreseeability and accessibility "*depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed*" (*Gillan and Quinton v. UK*, §77; *Hashman and Harrup v. the United Kingdom* [GC], §31; *S. and Marper*, §96).

65. As explained above, although the EI Code contained provisions relating to the exercise of the section 7 power, it also noted in terms that there was no statutory underpinning for those provisions and that they were treated as binding "*as a matter of policy*". That is a wholly inadequate set of arrangements in view of (a) the extreme breadth and potency of the powers in question, and (b) the fact that they are invariably exercised in secret. The breadth of the powers (which amount in principle to a general power on the part of the Secretary of State to authorise unlawful acts) makes it all the more essential that their application is rendered foreseeable and accessible by other safeguards and constraints. The secrecy with which they are necessarily exercised means that a "*policy*" is an unacceptable source of such safeguards and constraints: all it would take is for the policy to be inconsistently enforced, or indeed varied or disapplied, for the safeguards to be worthless.

66. Nor can any secret, internal, so-called "below the waterline" arrangements assist the UK in principle in meeting the requirements of foreseeability and accessibility. An accessible and foreseeable scheme under the Convention cannot be based on a secret set of unpublished guidance, not publicly available, not subject to any Parliamentary review or oversight. A clear and public regime for the use of CNE is required.

(iii) The CNE Section 7 Regime does not meet the "*quality of the law*" requirements of the Convention

67. In *Weber and Saravia v Germany* (2008) 46 EHRR SE5 (decided in 2006) this Court, when considering admissibility, identified the minimum safeguards for communications surveillance that must be satisfied to protect against arbitrary interference and abuse. The CNE regime does not satisfy the minimum requirements identified in *Weber*, for the reasons set out below. Further, and in any event, the *Weber* safeguards are no longer sufficient to address the level of unprecedented threat the impugned measure poses for privacy and security in a democratic society.

68. In its recent case law, the Court has made it clear that significant developments in electronic communications and covert surveillance capabilities must be matched by commensurate developments in the minimum legal safeguards applicable to the use of covert surveillance powers. In *Szabó* the Court noted that "*the mere existence*" of legislation authorising the monitoring of electronic communications "*involve[s], for all those to whom the legislation could be applied, a menace of surveillance*". (§53). At the same time, the Court highlighted that *"[g]iven the technological advances since the* Klass *case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely*" (§53, citing *Klass*, §41). In particular, the Court noted the "*remarkable progress*" in the scale and sophistication of surveillance technology and techniques in recent years, which have "*reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread*" (§68).

69. The Court explained that it was necessary, in light of these technological developments, to ensure "*the simultaneous development of legal safeguards securing respect for citizens' Convention rights*" (§68). Otherwise, the Court concluded, "*it would defy the purpose of government efforts to keep terrorism at bay [...] if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives*." (§68).

70. In *Szabó*, the Court stated that it was "*a matter of serious concern*" where "*broad-based*" legislation could potentially enable "*so-called strategic, large-scale interception*" (§69). The Court added, in this respect, that "the *possibility occurring on the side of Governments to acquire a detailed profile of the most intimate aspects of citizens' lives*

may result in particularly invasive interferences with private life" and made specific reference to "*views expressed by the Court of Justice of the European Union and the European Parliament*" (§70). The Court stressed accordingly that "*[t]he guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices*." (§70).

71. The points made by the Court in *Szabo* apply *a fortiori* to CNE, especially bulk CNE over material that its owners have chosen *not* to communicate over a public network. The *Weber* minimum criteria must apply as a minimum. The touchstone is whether the degree of interference with privacy is comparable to that involved in interception of communication. In *R.E. v. the UK* (§130), the Court held that "*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*" (cf. *Uzun v. Germany*, 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, and often far more so. Further, the Court should develop its minimum safeguards to reflect the exceptional intrusiveness of modern CNE techniques.

C. Absence of mandatory minimum safeguards

72. The six criteria laid down in *Weber* do not represent a mechanical set of rules for assessing whether a CNE regime is in accordance with the law (not least because they represent the measures which were thought to be necessary to secure the compliance with the Convention rights of a different and less intrusive form of surveillance). But they do provide a set of bare minimum standards. Merely meeting the *Weber* criteria is insufficient – especially in the light of the development of surveillance technology and the seriousness of the interference – to ensure there are sufficient safeguards for powers to be in accordance with the law. However, if bulk CNE powers do not even meet the *Weber* criteria, they will certainly be inadequate to and will constitute a violation of Convention rights.

73. In *Weber* (§95), the Court at 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."

(i) Prior to the publication of the draft EI Code in 2015

74. Prior to the publication of the draft Codes, or alternatively the formal promulgation of the EI Code in January 2016, the *Weber* minimum requirements were not satisfied. 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 to authorise activity that would otherwise be unlawful.

75. The availability of a warrant under a bare statutory power that simply cancels any unlawfulness is self-evidently not an adequate safeguard against arbitrary conduct. Such arrangements satisfy *none* of the *Weber* minimum criteria. Even the requirement for a limit on duration is not satisfied in respect of general authorisations that can be repeatedly renewed under a long-term rolling system of authorisations.

76. The fourth *Weber* criteria requires proper procedures for storage and use. These include proper arrangements for the protection of legally privileged material. In relation to material subject to legal professional or other privilege, the regime was particularly

defective. In *Belhaj*, GCHQ conceded that its procedures in relation to intercept of privileged material were not lawful. That concession was rightly made:

76.1 The definition of privilege in GCHQ's procedures is inadequate –it ignores litigation privilege. (*Belhaj*, §§14-16)

76.2 The guidance does not recognise that 'events', metadata and communications data may be privileged.[42]

76.3 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.

77. The Applicants submit that, prior to the publication of the first Draft EI Code in February 2015, the CNE Regime cannot be held to satisfy the "quality of the law requirements" of the Convention and, in particular, the requirements articulated by this Court in *Weber*.

(ii) After the publication of the first Draft Equipment Interference Code

CNE cannot meet the "quality of the law" requirements because it is operated under a bare power with no safeguards or Code of Practice

78. As the IPT rightly observed at (§49), the s.7 CNE Regime "*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***" (emphasis added)

79. Accordingly, both the draft 2015 EI Code and the 2016 EI Code state at (§1.4.):

> *"There is no power for the Secretary of State to issue codes of practice in relation to the powers and duties in section 7 of the 1994 Act. However, SIS and the Government Communications Headquarters ("GCHQ") should as a matter of policy (and without prejudice as to whether section 6 of the 1998 Act applies) comply with the provisions of this code in any case where equipment*

[42] Martin Witness Statement, Exhibit CM2-5 (GCHQ Reporting Policy – Sensitive Professions Dec 2010) para 5.

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."

80. The Applicants submit that the domestic regime fails to provide for adequate safeguards as there is no power for the Secretary of State to issue a binding code of practice in relation to s. 7 CNE. A mere reference to "*should… as a matter of policy*" fails to make up for the lack of a clear statutory framework, and therefore violated the "*in accordance with the law requirement*" of the Convention. There was no power for Parliament to consider whether special and extended provision needed to be made for large-scale CNE operations being conducted outside the British Islands, and a mere policy can be departed from whenever there is thought to be a good reason for doing so, in secret.

Even if the EI Codes were applied to s.7 CNE, they would still fail to satisfy the Weber mandatory minimum safeguards

81. Even if the EI Code did apply, the regime would still not comply with the *Weber* minimum criteria.

82. First, the EI Codes fail to indicate (still less control) the scope of the CNE Regime under s. 7 ISA. In *Centrum för rättvisa v. Sweden* (App. No. 35252/08, 19 June 2018), the Court noted that it is "*of further importance that signals intelligence conducted on fibre optic cables* ***may only concern communications crossing the Swedish border*** *in cables owned by a communications service provider.* Communications **between a sender and a receiver in Sweden may not be intercepted**, regardless whether the source is airborne or cable-based" (§122, emphasis added).

83. The legislative scheme is vague and uncertain, and of extraordinary breadth. 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:

    83.1 Section 5 ISA could be used to obtain the photos directly from the smartphone using CNE. This would require a Secretary of State warrant.

83.2 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]). If section 8(1) of RIPA is used, a Secretary of State warrant would be required.

83.3 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.

83.4 Section 7 ISA could be used to obtain the photos under GCHQ's broad, existing, rolling class authorisation for CNE abroad. No Secretary of State warrant is required, nor is there any equivalent certification procedure. GCHQ can authorise the obtaining of the photos internally. All of the key safeguards that are a crucial part of maintaining the lawfulness of the RIPA interception regime are absent.

84. In this scenario, the EI Code does not provide any substantial safeguard. It simply says:

> "*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.*"

85. David Anderson QC rightly observed that the Code "*does not elaborate on what factors should be taken into account in the course of that consideration*".[43] In contrast, other provisions of the Draft EI Codes are phrased in terms of "*should*" or "*must*".

86. 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.

87. Additionally, in *Centrum för rättvisa v. Sweden*, the Court held:

[43] A Question of Trust 6.33 or page 103.

"*It is further of relevance in this context that, in its 2010 and 2016 reports, the Data Protection Authority found no evidence that personal data had been collected for other purposes than those stipulated for the signals intelligence activities (paragraphs 59-60). In these circumstances, the Court is satisfied that the scope of application of the development activities is sufficiently demarcated.*" (§122)

88. The Applicants note that, according to the 2014 Annual Report of the Intelligence Services Commissioner:

88.1 SIAs reported 43 errors to the Commissioner, while 9 were discovered during his inspections.[44]

88.2 Of all the errors, the most common error was because of a failure to obtain authorisation in time.[45]

88.3 4 of these errors were the result of unauthorised interference with property.[46]

88.4 The commissioner "*expressed concern that the agencies did not report errors in a timely way*".[47]

89. In his 2015 Annual Report, the Intelligence Services Commissioner noted that there was a total of 83 errors which was "*quite a significant rise from the 43 errors of 2014*".[48]

D. Further minimum safeguards

90. The application in *Weber* was filed in 2000 and declared inadmissible (by a majority) in 2006. Since then, there have been "*seismic shifts in digital technology*" (*Carpenter v United States* 585 US _ (2018) at p.15, Roberts CJ).

91. It is therefore appropriate to review the principles to ensure that Convention rights remain effective. The same process is ongoing in apex courts across the world. For example, the CJEU has identified extensive minimum safeguards for communications data in *Digital*

[44] Report of the Intelligence Services Commissioner for 2014 (25 June 2015, HC 225) page 40.
[45] Ibid, page 41.
[46] Ibid, page 42.
[47] Ibid, page 45.
[48] Report of the Intelligence Services Commissioner for 2015 (8 September 2016, HC 459) page 49.

Rights Ireland and *Tele2/Watson*. In *Carpenter* at p.17, the US Supreme Court (per Roberts CJ) extended the protections of the Fourth Amendment to ensure that the prohibition on unreasonable searches and seizures remains effective in the modern world:

> *"cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society … [A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates [communications data], including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data … a comprehensive dossier of his physical movements."*

92. When the Court identified, in its *Weber* judgment, the minimum safeguards necessary in a regime for the surveillance of communications which is compliant with the Convention, many forms of modern communication were not in existence. Changes in technology, and the development of extremely invasive techniques such as CNE, mean that the safeguards require updating and developing, as the Court indicated was necessary in relation to interception in *Szabo*.

(i) No requirement for individual reasonable suspicion

93. In *Szabó* the Court noted the requirement of "*a sufficient factual basis for the application of secret intelligence gathering measures … on the basis of an individual suspicion regarding the target person*" as critical for "*the authorising authority to perform an appropriate proportionality test*" [§71]. Similarly, in Zakharov, the Grand Chamber held that the authorisation procedure "*must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security*". (§260).

94. As specified in the 2016 Code of Practice, authorisations issued by the Secretary of State "*under section 7 may be specific to a particular operation or user, or may relate to a*

broader class of operations." (emphasis added) (§7.6). When a broad class of operations is authorised – in other words conducting mass or bulk CNE over entire classes of device users, or large groups of people, no attempt is made to verify "*the existence of a reasonable suspicion against the person concerned*" as no person is identified.

95. Even where internal authorisation is sought under section 7, that authorisation focuses on the necessity and proportionality of a particular operation (2016 Code, §7.13), which may target numerous individuals and devices. No reasonable suspicion with regard to a particular person or device is required.

96. Proper grounds will exist for using CNE against a target only where there are reasonable grounds for suspicion of the person about whom information is sought (see *Zakharov*, §260). This test is well understood in the context of search warrants and arrest.

97. Compounding the harm caused by the lack of a reasonable suspicion, there is also no requirement to filter data obtained under section 7.[49] The Intelligence Services Commissioner encouraged the use of such filtering: ("*I stressed to [GCHQ] the importance I place on filters which help avoid any unnecessary intrusion*").[50] Yet the Code contains no such obligation.

98. Second, in Big Brother Watch, the Court highlighted that "*the search criteria and selectors used to filter intercepted communications should be subject to independent oversight*". (§346). There is no such requirement in the EI Code.

99. This failure to filter and to conduct specific oversight of the search criteria and selectors used is similar to the failure to apply selectors to communications collected in bulk which was identified and critiqued by this Court in *Big Brother Watch v. United Kingdom*. The Court went on to find a violation of Article 8 of the Convention based on (§387):

> *"first, the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for*

[49] The Applicants presented their position on filtering to the IPT (see Applicants' Skeleton Argument §59(d) and (e)), contrary to the Government's assertion otherwise ((Government Observations, §132).
[50] Report of the Intelligence Services Commissioner for 2014 (25 June 2015, HC 225) page 25.

examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination."

(ii) No prior independent authorisation

100. In *Weber,* a cross-party and independent commission of the German Parliament approved surveillance and the selectors applied. The Court repeated the principles in *Szabó*: "*in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exceptions, warranting close scrutiny … supervision by a politically responsible member of the executive, such as the Minister for Justice, does not provide the necessary guarantees"* [§77]. The same approach was taken by the Grand Chamber of the CJEU in *Digital Rights Ireland* [§62] and *Tele2/Watson* [§120].

101. There is no meaningful scrutiny involved in the grant of a rolling section 7 authorisation to carry out CNE abroad. A general authorisation to carry out CNE abroad is unlikely to represent a real check or control on such operations by the Secretary of State. In particular, authorisation by the Secretary of State is neither judicial nor independent. In *Zakharov* §258 the Court referred to approval of of authorisation by a non-judicial authority "*provided that that authority is sufficiently independent from the executive*."

102. Such limited pre-authorisation is not remedied by the UK's post-authorisation oversight for the following reasons:

    102.1 The IPT does not provide an adequate remedy for the absence of prior judicial authorisation. It may only consider a case referred to it. The Commissioner lacks power to refer a case to the IPT and is not permitted to notify a victim of excessive or unlawful interception. The Independent Reviewer found this "*hard to understand*".[51] It is difficult to see any rational justification for imposing such a restriction, which is of blanket effect in all cases including those where notifying the victim would have no adverse impact on national security. Its effect is that the only means by which the IPT could even conceivably remedy problems in the initial grant of warrants would be for large numbers of individuals to make speculative claims to the IPT, asserting secret, unknown

[51] A Question of Trust, para 14.104.

and undefined problems with the warrant process. Even that approach would be ineffective because the IPT would reject such claims: *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15_165-CH §§47-48.

102.2 The Commissioner's oversight has in the past been ineffective. For example:

102.2.1 The Commissioners all failed to identify the defects in the Agencies' procedures related to legally privileged material that led to the concession in *Belhaj*.

102.2.2 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,[52] after the initiation of the claim brought by the Applicants. The GCHQ Witness'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*").[53]

102.2.3 It does not appear that there is any oversight of individual selectors or other filtering mechanisms to ensure that they work effectively, properly and proportionately.

103. While the First Section in *BBW* concluded that prior judicial authorisation was "*highly desirable*" but not a "*necessary requirement*" under Article 8 "*in view* [of] *the pre-authorisation scrutiny ... extensive post authorisation scrutiny provided by the (independent) Commissioner's office and the IPT and the imminent changes to the impugned regime*" [§§318, 381], one of the Applicants in this case, Privacy International, has joined the other applicants in *BBW* in asking the Grand Chamber to depart from that finding.

(iii) No requirement for subsequent notification of CNE

[52] Martin Witness Statement, §71I.
[53] Martin Witness Statement, §71I.

104. Both the Court (in *Szabó* at §86 and *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, no 62540/00, 28 June 2007, §91) and the CJEU (in *Watson* at §121) recognise the importance of this safeguard, to enable those affected by CNE to be aware of the interference with their rights and to seek remedies against any abuse of the relevant surveillance powers.

105. The First Section in Big Brother Watch held that "*'subsequent notification' assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime*" [§317].[54] This fails to distinguish between the initiation of a bulk interception or bulk CNE operation and the subsequent storage, processing and use of information, where targets are presumably identified. If notification would not cause substantial harm to the public interest, it should be given. Other bulk interception schemes (eg in *Weber* and *Rättvisa*) do make provision for notification.

(iv) No requirement to guarantee the security and integrity of IT infrastructure and devices, as well as confidentiality of data

106. The Convention does not only impose obligations on states to abstain from interfering with individuals' rights. It also imposes positive obligations on public authorities to secure the rights enshrined in the Convention.[55]

107. In order to ensure that the rights guaranteed by the Convention are effectively safeguarded against abuse, the Court has clarified that "*although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life*". (*K.U. v. Finland*, §42).

108. The meaningful exercise of the Convention right to privacy is linked to the security of the devices, networks and services individuals rely on to communicate with each other. Accordingly, the security implications of surveillance measures such as CNE are relevant

[54] One of the Applicants, Privacy International, is also challenging this finding before the Grand Chamber.
[55] The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights, Alastair Mowbray 2004 page 186.

to an assessment of the scope and nature of that measure's interference with the right to privacy.

109. The U.N. Special Rapporteur on Freedom of Expression has explained that individuals exercise their right to privacy by communicating in a manner that is "*private*" and "*secure".*[56]

110. In his intervention before this Court, the U.N. Special Rapporteur for Freedom of Expression underlined (§6) that Governments "are obligated to take specific measures to guarantee protection of the law". At (§14) he goes on to say:

> "*In addition to obligations to provide a comprehensive legal framework to protect privacy, States have an obligation not to intrude on privacy themselves and also a resulting obligation to protect the privacy of individuals from third-party hackers […] For example, encryption software allows individuals to protect data from digital surveillance by scrambling data to ensure that only intended recipients can actually access it. In response, States often make concerted efforts to prevent encryption, effectively eliminating the most operational safeguard of digital security. Releasing encrypted information can expose vulnerabilities in encryption, allowing third-party hackers access to the encrypted information. States should consider this security risk in implementing safeguards and access to remedy.*"

111. In their intervention (§11), Mozilla expressed their serious concerns about "*the harmful impact of state CNE on end- user security and its inherent corollaries, privacy and freedom of expression and access to information online; as well as on the integrity of the Internet-connected infrastructure on which society has come to rely*". This is because:

    111.1 CNE, by its very nature, relies on vulnerabilities that "*potentially affect all users of a service or software, even if the CNE is intended for only a small number of individuals*". (§12). Increasing device connectivity and the globalised nature of the Internet allows users to store information on cloud services, not only contribute to the far-reaching effects of CNE, but also make it impossible "*to*

[56] Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/23/40, 17 April 2013), para 23.

guarantee that a vulnerability is used only within or outside certain jurisdictions". (§13-14).

111.2 CNE can leave sensitive personal data and infrastructure open to abuse. It permits access to extremely sensitive information. For example, the current UK Equipment Interference Code of Practice gives examples of the kinds of information to which use of CNE could allow access; *"every keystroke entered by users";* passwords; photographs; the location of meetings in calendar appointments; the content, sender and recipient of stored emails; and video surveillance footage.' That list will only increase as more and more devices are network-enabled. This allows for such sensitive data, infrastructure and services to "*logically also be accessed or interfered with by anyone else with knowledge of that same vulnerability (or even possession of the government's own CNE tools)—for example, cybercriminals and other malicious actors*". (§18).

112. 135. Fundamental security concerns were also raised by Professor Ross Anderson, in his Expert Report before the IPT Proceedings, where he highlighted that the intrusion caused by CNE:

> "*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 service. 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… 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 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 hack).*" (§21-22).

113. Taking into account the obligations of states to maintain the integrity and security of information systems, so that individuals can effectively exercise their fundamental rights, inducing CNE measures that undermine the security of systems is not compatible with human rights law. CNE, in such circumstances, contradicts states' obligations to guarantee individuals' privacy, by implementing measures that would protect the security, integrity and confidentiality of information technology systems. By their very nature, CNE is the exact opposite; a continuous undermining of the security upon which effective practical protection of the Convention right to privacy depends.

E. The UK's Bulk CNE regime is unnecessary and disproportionate

114. The Court has rightly identified the necessity and proportionality of the section 7 regime to be of relevance *proprio motu* and invited parties to file observations on this.

(i) The test: "strict necessity"

115. In *Klass*, the Court held that "*[p]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions*". (§42).

116. In *Szabó* the Court further clarified that in the context of covert interception of electronic communications the requirement of necessity under Article 8(2) imposes a test of strict necessity "*in two aspects*." First, a secret surveillance measure must be "*strictly necessary, as a general consideration, for the safeguarding the democratic institutions*". Second, it must be "*strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation*." The Court explained that "*any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal*." (§73).

117. In considering whether the test of strict necessity is satisfied, the existence of safeguards is a necessary, but not sufficient, condition.

118. In *Szabo*, the Court cited and drew support from some of the recent CJEU jurisprudence. In *Digital Rights Ireland*, the CJEU held that "*Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to*

ensure that it is actually limited to what is strictly necessary", (§65) as it "*covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*". (§57).

119. Similarly, in *Schrems* the CJEU held that legislation is not limited to what is strictly necessary when it equally:

> "*authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.*" (§93).

120. The utility of a particular surveillance measure is likewise a relevant, but not conclusive, consideration. As the Independent Reviewer observed in his 2015 report, even if bulk interception makes a "*valuable*" contribution to protecting national security, "*[i]t does not of course follow that it is necessarily proportionate*".[57] Indeed, the Independent Reviewer in his 2016 report on bulk powers explicitly noted that he was not *"asked to opine on...whether the safeguards contained in the [Investigatory Powers] Bill are sufficient to render them proportionate for the purposes of the European Convention on Human Rights"*.[58]

(ii) Bulk or large-scale CNE is neither strictly necessary nor proportionate for the safeguarding of democratic institutions and individuals' privacy

121. As a surveillance technique, CNE is unprecedentedly intrusive. As underlined above (for example at paragraphs 6 and 30), CNE activities can provide constant access to the most intimate aspects of their private lives, as authorities are able to in real time infiltrate a person's privacy by accessing uncommunicated photos, videos, diaries, notes and any

[57] A Question of Trust, para 7.26.
[58] Report of the Bulk Powers Review, para 1.11(b). Reply Annex No. 32.

other sensitive information stored on their device, as well as covertly utilising microphones, cameras and GPS-tracking.

122. However great the intrusion when CNE is undertaken on a targeted basis, it is very much greater when it is undertaken in bulk, i.e. on a large scale and without specific justification by reference to the circumstances of a particular intrusion. Bulk CNE is a core aspect of UKSIS's CNE activity, as confirmed in a letter from the Minister of State for Security and Economic Crime to the Chair of the Intelligence and Security Committee on 3 December 2018 in which he wrote that GCHQ had concluded that it was "*necessary*" to conduct "*a higher proportion of ongoing overseas focused operational activity using the bulk EI regime than was originally envisaged*".

123. When such intrusive activities are authorised in bulk, or by reference to types of activity rather than specific, targeted actions, they are not strictly necessary for the achievement of any legitimate purpose. A 'bulk' approach necessarily involves a departure from any case-by-case consideration of whether or not it is necessary for an unlawful or tortious act to be performed. That can be illustrated by the fact that, as of 2015, only five class authorisations were in place to cover all of GCHQ's foreign intelligence activities including (but presumably far from limited to) CNE. Very large numbers of intrusions will have been permitted under each of these authorisations. Such generalised authorisations for such incredibly intrusive activity cannot possibly allow for sufficient consideration of whether each intrusion is "*strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation*." Szabo (§73). In other words, at the point at which any given CNE act takes place, the relevant exercise of the section 7 power which renders it lawful rather than criminal may have occurred some considerable time beforehand and without any regard whatsoever to the particular circumstances of the case.

124. When determining whether an interference with the right to privacy was "*necessary in a democratic society*", the Court examines whether the interference was proportionate to the aims pursued. This necessarily involves a balancing exercise between competing interests.[59] In *Leander*, the Court noted that "*national authorities enjoy a margin of*

[59] ECtHR, *Z v. Finland* (App. No. 22009/93, 25 February 1997), para 94.

appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved". (§59).

125. The Court has recognised on numerous occasions that blanket or indiscriminate measures that seriously interfere with privacy may not be justified. In *S and Marper*, the Grand Chamber held that the collection and retention of DNA and fingerprints of innocent people was contrary to Article 8. In particular, the Grand Chamber was "*struck by the blanket and indiscriminate nature of the power of retention in England and Wales*", noting that "*[t]he material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken—and retained—from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences*" (§119).

126. It further noted that retention was "not *time limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected*" and a lack of safeguards to ensure that material was deleted "*according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances*" (§119).

127. The Grand Chamber concluded that "*the blanket and indiscriminate nature of the powers of retention...fails to strike a fair balance between the competing public and private interests*" (§125). It held that the UK had "*overstepped any acceptable margin of appreciation in this regard*" even though the DNA database was undoubtedly a valuable tool for detecting and prosecuting serious criminals (§125).

128. Similarly, in *MK v France*, the Court held that the French national digital fingerprint database was unlawful. In doing so, it rejected the arguments of the French court that "*retaining the fingerprints was in the interests of the investigating authorities, as it provided them with a database comprising as full a set of references as possible.*" (§13). The Court also noted that the need for safeguards *"is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes*" (§32). It warned that the logic of the French government's arguments "*would in practice be tantamount to justifying the storage of*

information on the whole population of France, which would most definitely be excessive and irrelevant".

129. As in *Marper* and *MK*, the Government claims the power to carry out CNE in bulk in relation to millions of individuals without any individual reasonable suspicion that they have committed or are committing a criminal offence or are engaged in an act amounting to a specific threat to national security. This interception is "*blanket and indiscriminate*" and is no less intrusive because it "*undergo[es] automatic processing*" (in fact, the opposite is true – the availability of sophisticated search and processing tools makes holding a large quantity of data more intrusive because it can be rapidly analysed).

130. The present case should be in any event be distinguished from the judgment of the First Section in Big Brother Watch, where the Court held that bulk interception of communications data could be necessary for security operations. That case is currently pending before the Grand Chamber. In any event, the regime under consideration in that case contains a number of safeguards for bulk use of data not present in respect of CNE set out above.

(iii) The security implications of the UK's CNE regime also renders it disproportionate

131. The ISC Report of 12 March 2015, one of the few publicly-available sources about the extent of the use of the section 7 power in practice (which is itself heavily redacted), states:

> *"182. We asked GCHQ how they balance the potential intelligence benefits against the inherent security risks ***. GCHQ explained that they have an Information Assurance role, providing government, industry and the public with advice and guidance to protect their IT systems and use the internet safely, ***. Nevertheless, GCHQ said that "*** our goal is to be able to read or find the communications of intelligence targets". The Committee questioned whether this work exposed the public to greater risk.*
>
> *183. In terms of software vulnerabilities, GCHQ explained that "the lion's share of vulnerabilities *** are publicly known... [but] vendors haven't yet released a fix for them or, if they have, many users are slow to apply the fix".*

*In terms of scale, they explained that "around 10,000 vulnerabilities in common security products were discovered [globally] and publicly logged last year". GCHQ themselves discovered a number of vulnerabilities (***) which were reported so that vendors could improve their products. Of these ***."* [60]

132. The Applicants infer that the redacted parts of the ISC's report explain GCHQ's practice of hoarding security vulnerabilities rather than reporting them so they can be repaired. What recent cyberattacks have underlined is that hoarding system vulnerabilities has dangerous consequences for citizens globally. In December 2015, for example, hackers were able to successfully compromise IT systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to at least 230 thousand end consumers.[61]

133. In a leaked document that was produced by the National Cyber Security Centre (NCSC), it was reported that "*due to the use of wide-spread targeting by the attacker, a number of Industrial Control System engineering and services organisations are likely to have been compromised*". The report said that "*these organizations are part of the supply chain for UK critical national infrastructure, and some are likely to have remote access to critical systems*".[62]

134. Another illustrative example of the dangers of CNE is the WannaCry attack. WannaCry was developed by hackers who effectively managed to exploit vulnerabilities stockpiled by the United States National Security Agency (NSA),[63] and seriously impacted European infrastructure operators in the sectors of health, energy, transport, finance and telecoms.[64]

135. Germany and the United Kingdom were among the first countries where the WannaCry malware attack was reported. According to the Berlin public prosecutor's office, the

---

[60] Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework (12 March 2015) 68-69.

[61] Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid' (Wired, 3 March 2016) available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[62] Joseph Cox, 'GCHQ Says Hackers Have Likely Compromised UK Energy Sector Targets' (Vice 17 July 2017) available at: https://www.vice.com/en_us/article/9kwg4a/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets

[63] Alex Hern, NHS could have avoided WannaCry hack with 'basic IT security', says report (The Guardian, 27 October 2017) available at: https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office

[64] EU Agency for Fundamental Rights (FRA), Fundamental Rights Report 2018 available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf, 161

WannaCry attack resulted in a total of 450 Deutsche Bahn computers being affected.[65] In the United Kingdom, the WannaCry cyberattack had potentially serious implications for the National Health Service, leading to widespread disruption in at least 81 of 236 hospital trusts in England, with 19,000 medical appointments being cancelled, computers at 600 general practitioner surgeries being locked, and five hospitals having to divert ambulances elsewhere.[66] This potentially resulted in chaotic situations for patients, with sensitive personal data being encrypted or destroyed by the malware.[67]

136. This demonstrates that hoarding vulnerabilities can also seriously impact the security of government IT infrastructure as well. On 12 August 2019, in what was suggested to be an exploitation of security vulnerabilities, hackers leaked 700 GB of data obtained from the government of Argentina, "*including confidential documents, wiretaps and biometric information from the Argentine Federal Police, along with the personal data of police officers*".[68]

IV. VIOLATION OF ARTICLE 10

137. The role played by human rights organisations – such as the Applicants – is similar to the watchdog role of the press. (*Társaság a Szabadságjogokért* v. Hungary, App. no. 37374/05, 14 April 2009, §27; *Riolo v. Italy*, App. no. 42211/07, 17 July 2008, §63; *Vides Aizsardzības Klubs v. Latvia*, App. no. 57829/00, 27 May 2004, §42).

138. In general terms, the Section 7 regime contravenes Article 10 for the same reasons that it contravenes Article 8. Indeed, insofar as journalistic materials, or other equivalent material held by NGOs is interfered with, the case under Article 10 ECHR is *a fortiori*. The same applies when private expressions of political belief or other protected

[65] Chris Graham, Cyber attack hits German train stations as hackers target Deutsche Bahn (The Telegraph, 13 May 2017) available at: https://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/ ; see also Markus Böhm, 'Experten über "WannaCry"-Attacke: "Wir hatten noch Glück"' (16 May 2017) available at: https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html

[66] UK, National Audit Office, Department of Health, Investigation: WannaCry cyber-attack and the NHS (Report by the Comptroller and Auditor General, 27 October 2017) available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[67] Patrick Sawer, Robert Mendick, Stephen Walter, Nicola Harley, NHS cyber chaos hits thousands of patients (The Telegraph, 13 May 2017), available at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-chaos-hits-thousands-patients/

[68] Eugenia Lostri, 'Hackers Leaked Sensitive Government Data in Argentina – And Nobody Cares' (Lawfare 21 August 2019) available at: https://www.lawfareblog.com/hackers-leaked-sensitive-government-data-argentina-and-nobody-cares

categories of expression are interfered with by CNE, given the inevitable and serious chilling effect on freedom of expression that will result.

139. In *Catt v UK,* the Court noted:

> "*In the first place it considers significant that personal data revealing political opinion falls among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 58-60 and 67-70 above and S. and Marper, cited above, § 76). […] the Court considers that the nature of the applicant's complaint meant that the sensitive nature of the data in question was a central feature of the case both before the domestic courts as well as before this Court.*" (§112).
>
> "*the decisions [of the police] to retain the applicant's personal data did not take into account the heightened level of protection it attracted as data revealing a political opinion, and that in the circumstances its retention must have had a "chilling effect".*" (§123).

140. It is also because of this chilling effect that CNE constitutes an a particularly disproportionate interference with Article 10 rights under the Convention.

141. Second, it is not only the content of communications or communications data that can be targeted by the CNE regime; this activity enables also the constant, covert and real-time access and acquisition, destruction, alteration, extraction and in general processing of data that the user might not have wanted to communicate and merely wished to store on their device.

142. Third, the gathering of information is an "*essential preparatory step in journalism and an inherent, protected part of press freedom*" (*Satakunnan Markkinaporssi Oy v Finland*, §128). The Court has repeatedly emphasised that the protection of journalistic sources and journalistic material is a fundamental guarantee afforded by the right to freedom of expression. The same principles apply in respect of human rights NGOs engaged in the gathering of information in the public interest.

143. The concept of a journalistic source has been given a very broad definition by the Court. In *Telegraaf Media Nederland Landelijke Media BV v Netherlands*, the Court held that

"[a] journalistic source is any person who provides information to a journalist" and that "information identifying a source include[s], as far as they are likely to lead to the identification of a source, both the factual circumstances of acquiring information from a source by a journalist and the unpublished content of the information provided by a source to a journalist" (§86).

144. Article 10 protection extends not only to protection of journalistic sources but also to journalistic material including "*research material*" (see *Sanoma*, App. No. 38224/03, 14 September 2010 [GC], §§65-66; *Nordisk Film & TV A/S v Denmark* (Admissibility), App. No. 40485/02, 8 December 2005). *Sanoma* was itself concerned with access to journalistic material, not measures to identify a journalistic source. In *Nordisk Film & TV A/S v. Denmark*, the Court accepted the possibility that the compulsory handover of research material might have a chilling effect on the exercise of journalistic freedom of expression and was therefore in breach of Article 10.

145. The Court has repeatedly held that, given the fundamental importance of press freedom, any interference with journalistic information and, in particular, the right to maintain the confidentiality of sources, "*must be attended with legal procedural safeguards commensurate with the importance of the principle at stake*" (*Sanoma*, §88). Accordingly, Article 10 imposes specific and exacting requirements where a measure is capable of identifying journalistic sources and/or revealing journalistic material over and above those that apply under Article 8 and Article 10 generally.

146. Consistent with this case-law, this Court held in *Big Brother Watch* that "*the interference [with Article 10 rights] will be greater should [a journalist's] communications be selected for examination and [such selection] will only be 'justified by an overriding requirement in the public interest' if accompanied by sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination*" [§492].

147. The Court also made clear that special safeguards must apply at the least where the material of a journalist is sought or where there may be collateral intrusion [§499]. The Applicants invite the Court to endorse this approach in relation to journalists and, in addition, other "*public watchdog*" organisations including human rights NGOs.

148. In *Sanoma*, the Grand Chamber set out minimum safeguards which must be present to ensure that measures whose application is capable of identifying journalistic sources and/or revealing journalistic material are in accordance with the law (the "*Sanoma* Safeguards"):

148.1 First, "*is the guarantee of review by a judge or other independent and impartial decision-making body*", which is "*impartial*" and "*separate from the executive and other interested parties*" [§§90, 92]. The authorising body must not be an official or institution "*defending interests potentially incompatible with journalistic source protection*" [§93].

148.2 Secondly, the review must be *ex ante*, ie, before the relevant measure is implemented [§90]. This is because "*the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality*" [§91]; and see *Telegraaf Media* at §99-102, applying *Sanoma*. The Court's caselaw on the need for *ex ante* independent authorisation is clear.

148.3 Thirdly, the independent body must be "*invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not*" [§90] and it must "*be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be properly assessed*" [§92].

149. Crucially, the section 7 CNE regime does not provide for any *ex ante* independent, let alone judicial, authorisation at any stage, even where activities authorised are for the purpose of identifying journalistic sources. The applicants submit that the absence of this fundamental safeguard is alone sufficient to mean that the regime is not in accordance with the law under Article 10 on existing authorities.

150. Third, the Court has held that with regard to the freedom to hold opinions, which is an absolute right and a necessary condition for the exercise of freedom of expression,[69] individuals have the right not to be compelled to communicate their opinions.[70] As currently envisioned, there are no safeguards within the section 7 regime to prevent the communication of opinions that could be stored on targeted devices. Indeed, CNE is unique in that is gives access to its targets most intimate thoughts, including notes, documents and other indications of opinions which may never have been communicated (in contrast to interception, which targets communicated material).

V. VICTIM STATUS

151. The Applicants are victims within the meaning of Article 34 of the Convention.

152. In considering the scope of legislation permitting secret surveillance measures, the Court's consistent case law requires consideration of whether "*the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted*." (*Zakharov*, §171).

153. Two of the Applicants, Privacy International and Chaos Computer Club, engage in as human rights NGOs and campaigning groups. Privacy International has several times exposed overreaching state and corporate surveillance, with a focus on the sophisticated technologies and weak laws that enable serious incursions into privacy. It investigates, litigates, advocates, and educates in countries across the globe and has brought proceedings which, among others, resulted in surveillance laws being declared unlawful -most recently both the bulk interception regime and the regime for obtaining communications data from communications service providers violated Articles 8 and 10 of the Convention.[71]

[69] The Council of Europe Committee of Ministers has stated that "*any restrictions to this right will be inconsistent with the nature of a democratic society*", Report of the Committee of Ministers, in Theory and Practice of the European Convention on Human Rights, Van Dijk and Van Hoof, Kluwer, 1990, page 413.
[70] See, for example, ECtHR, Vogt v. Germany, App. No. 17851/91, 26 September 1995.
[71] 10 Human Rights Organisations v. United Kingdom, Application No. 24960/15 (13 September 2018). See also Privacy International, CJEU, C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others; IPT, Privacy International and Ors v. Secretary of State for Foreign and Commonwealth Affairs and Ors, IPT/17/86 & 87H.

154. Privacy International further works on capacity building on issues of privacy in developing countries, sometimes in places with weak democracies which are of particular interest to the UK and UK foreign policy, and where strong privacy safeguards may conflict with the objectives of intelligence and security agencies. Also, groups and individuals as well as activists in repressive regimes, individuals in the UK concerned about their own privacy, as well as victims, whistle-blowers, members of parliament, lawyers, whistle-blowers 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.

155. Specifically, following the Snowden revelations and during the course of judicial proceedings brought by Privacy International and other organisations before the IPT in 2014, it was discovered that the email communications of The Legal Resources Centre, an organisation based in South Africa founded by a Chief Justice of the Constitutional Court of South Africa, were intercepted and selected for examination pursuant to s.8(4) of RIPA, as well as of Amnesty International were unlawfully intercepted and retained by GCHQ. NGOs and those they assist are likely to be of interest to the UK intelligence services, as these examples show. Indeed, other claimants may also have had their communications intercepted. The only examples known are those where the interception was unlawful.

156. Moreover, in September 2018, MI5 admitted that it captured and read Privacy International's private data as part of its Bulk Communications Data (BCD) and Bulk Personal Datasets (BPD) programmes, which hoover up massive amounts of the public's data. This was once again disclosed during proceedings brought by the Applicants before the IPT. Privacy International's operations are clearly of interest to the UK intelligence services. A remedies hearing is currently pending before the UK IPT about these interferences, the scope and extent of which are currently unknown.

157. The rest of the Applicants submit that they are also likely to be affected by the CNE regime, in their capacity as providers of computer and internet services. The documents disclosed by former NSA contractor Edward Snowden illustrate that the GCHQ had

targeted telecommunications companies such as Deutsche Telekom AG,[72] Netcologne,[73] and Belgacom;[74] Satellite operators like Stellar, Cetel, and IABG,[75] or companies that facilitate encryption for mobile phones like Gemalto,[76] Giesecke and Devrient.[77] Any infrastructure operator is likely to be a target for CNE.

158. Second, the IPT rightly concluded, in the present case, that the Applicants satisfied the requirement of victim status and proceeded to determine the case.

VI. JURISDICTION

159. The Applicants note that the question of jurisdiction was not important in the IPT proceedings because, under the EI Code, regardless of whether or not the Article 1 test of jurisdiction was satisfied, the UK Government applied the Convention as a matter of policy to all usage of s. 7 to conduct CNE.[78] The IPT has jurisdiction under section 65 of the Regulation of Investigatory Powers Act 2000 to consider a breach of a policy by the UK Intelligence Services as well as a claim that the Convention has been breached. Therefore, a breach of the EI Code would result in a claim under domestic law; the question whether the Convention is engaged would not play a significant role. As a result, the parties only considered examples of the question of jurisdiction before the IPT.

160. Before this Court, the UK contends that there is no jurisdiction to consider CNE operations carried out outside the UK. This is incorrect. CNE operations under section 7 are within the Article 1 jurisdiction of the Convention:

161. First, CNE, involves tampering with devices to extract information. That information will then be retrieved and provided to the UK Intelligence Services, in the UK. Once it

[72] 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/
[73] Ibid.
[74] 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/
[75] 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/
[76] 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/
[77] Ibid.
[78] Para 7.1of the EI Code states: 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.

arrives in the UK, the private information will no doubt be processed, read and analysed, then stored and further distributed and reported upon in the UK. All these activities involve substantial interferences with privacy within the UK. Indeed, the whole purpose of using CNE is to take information, provide it to the UK Intelligence Services in the who, who can then analyse and exploit it.

162. This is the approach taken by the First Section in Big Brother Watch (§421), where it held that, in the context of intelligence sharing from a nonCouncil of Europe member state to a Council of Europe one "*[t]he interference lies in the receipt of the intercepted material and its subsequent storage, examination and use by the intelligence services of the respondent State*". Applied to CNE, once the CNE obtained data is received by the UK intelligence services, stored, examined or used, there has been an interference with privacy to which the Convention applies.

163. Secondly, by carrying out CNE, the UK remotely exercises de facto effective control over the equipment being interfered with and engages the jurisdiction of the Convention.

164. Under Article 1 of the Convention, a state's jurisdictional competence is primarily territorial (Banković and Others, §§ 61 and 67). Conversely, acts that are performed or produce effects outside a contracting state party's territory can exceptionally constitute an exercise of jurisdiction under Article 1. In its case-law the Court has recognised a number of exceptional circumstances capable of giving rise to the exercise of jurisdiction by a Contracting State outside its own territorial boundaries.

165. In *Loizidou*, the Court stated:

> "*Bearing in mind the object and purpose of the Convention, the responsibility of a Contracting Party may also arise when as a consequence of military action - whether lawful or unlawful - it exercises effective control of an area outside its national territory. The obligation to secure, in such an area, the rights and freedoms set out in the Convention derives from the fact of such control whether it be exercised directly, through its armed forces, or through a subordinate local administration.*" (§62)

166. In Al-Skeini, the Court further articulated:

"*Where the fact of such domination over the territory is established, it is not necessary to determine whether the Contracting State exercises detailed control over the policies and actions of the subordinate local administration. The fact that the local administration survives as a result of the Contracting State's military and other support entails that State's responsibility for its policies and actions.*" (§138)

167. The same approach applies where a Contracting State exercises effective physical control over a person, even in territory that is not controlled by a Contracting State. This approach leads to a straightforward application of the Convention to foreign CNE.

168. For example, assume that Google, operates a large facility containing thousands of computer servers in Ireland. GCHQ decides to carry out CNE, penetrating the whole of Google's Irish infrastructure, enabling it to collect, exporting, and proces of the data contained within those systems. These activities amount to de facto effective control over that infrastructure. Having secured electronic control over the infrastructure, the position is no different to a detainee or particular premises being seized by British armed forces.

169. In addition, the duration of control is not brief or limited. As the GCHQ admitted in the course of the IPT Proceedings, it carries out "persistent hacking operations (where an implant resides on a computer for an extended period)", (IPT Judgment of 12 February 2016, §5). CNE operations are an important tool for GCHQ to secure long term and effective control over IT infrastructures and devices.

170. The Snowden documents offer useful example. GCHQ had carried out CNE over Belgacom's networks (Belgium's largest telecommunications provider),[79] which serves millions of people across Europe.[80]

171. Moreover, it was reported that the GCHQ managed to get access not only to Belgacom's internal employee's computers, but was also able to gain control over the encrypted and unencrypted streams of private communications handled by the company for its

[79] 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.
[80] Gallagher, R. (13 December 2014) Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, The Intercept, https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/.

customers.[81] The CNE activity was reported to have lasted from 2010 to 2013, an extended period under which GCHQ had practical control of Belgacom's computer systems.

172. The Applicants submit that this is an illustrative and realistic example of how the GCHQ can obtain effective, constant/continuous and persistent control over IT infrastructure located outside the UK; an act which has severe implications for millions of users located across the globe and which triggers the extra-territorial applicability of the Convention.

VII. EXHAUSTION OF DOMESTIC REMEDIES

173. The Applicants have exhausted their domestic remedies and their application should be declared admissible. They invite the Court to reject the objections raised by the Government on the following grounds:

174. First, in its settled case-law, the Grand Chamber has explained that "*the rule of exhaustion is neither absolute nor capable of being applied automatically; for the purposes of reviewing whether it has been observed, it is essential to have regard to the circumstances of the individual case*". (*D.H. and Others v. Czech Republic*, §116). The Grand Chamber has further recognised that the rule "*must be applied with some degree of flexibility and without excessive formalism*" (*Azinas v. Cyprus*, §38; *Fressoz and Roire v. France*, §37; *Scoppola v. Italy* (no. 2), §69).

175. Secondly, the the availability of the remedy should be judged at the time an application is filed with the Court. This approach was confirmed by the Court in BBW with respect to the applicants in the first and second of the joined cases. The Court accepted that "*at the time* [they] *introduced their applications, they could not be faulted for relying on* Kennedy *as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime*". (§268, emphasis added)

176. Thirdly, the relevant question is not whether there were theoretically further steps which could have been taken to pursue the claim domestically, but whether in practice there was an effective domestic remedy which could be seen to have reasonable prospects of success: Applications 8319/07 and 11449/07 *Sufi and Elmi v United Kingdom,* §208. In

[81] A Question of Trust, Annex 7, para 16.

that case, an applicant had been advised by specialist counsel that an application for reconsideration of an immigration application would be unsuccessful, and as a result no such application was made before an application was made to the European Court of Human Rights. The Court rejected a submission that the applicant had failed to exhaust domestic remedies.

177. Applying those principles to the present case, the position is that the Applicant exhausted their domestic remedies to the extent that could reasonably have been expected. In particular:

177.1 At the time when the application was lodged, the Government's firm position was that there was no domestic route by which to appeal against or challenge a decision of the IPT. That position was upheld by the Divisional Court and the Court of Appeal. Only recently has the Supreme Court confirmed that judicial review is in fact available, but it was very far from clear at the time of the application that that would be the ultimate outcome (and the Government argued throughout the proceedings that it should not be).

177.2 Further, although the result of that Supreme Court decision is that there are judicial review proceedings ongoing in England & Wales arising out of the decision of the IPT, those proceedings (as explained in the Applicants' letter of 16 October 2019) concern different issues from those raised by these proceedings. They are concerned with a different statutory power, namely section 5 of the Intelligence Services Act 1994, which concerns activity within the United Kingdom. The subject matter of this Application is section 7 of the same Act, which (principally) concerns activity outside the United Kingdom. The Government correctly notes in the first paragraph of its Observations that the present Application "*is solely concerned with the lawfulness of the regime governing CNE activity outside the UK [...] under section 7 of the Intelligence Services Act 1994*" and raises no issue about the legal regime governing the use of section 5.

177.3 Further, (i) the judicial review proceedings are concerned to a large extent with the interpretation of domestic law, and (ii) they are being pursued only by Privacy International and not by the other Applicants.

178. In addition, , as explained at paragraphs 159 to 172 above, the present proceedings raise issues of jurisdiction which in practice could *only* be determined in this Court. Applying the principles in *R (Ullah) v Special Adjudicator* ([2004] 2 AC 323) the UK courts rarely seek to develop the Convention jurisprudence in this area, considering it properly a matter for the ECtHR. As Lord Bingham put it (§20):

> *"While [ECtHR] case law is not strictly binding, it has been held that courts should, in the absence of some special circumstances, follow any clear and constant jurisprudence of the Strasbourg court: R (Alconbury Developments Ltd) v Secretary of State for the Environment, Transport and the Regions [2001] UKHL 23, [2003] 2 AC 295, paragraph 26. This reflects the fact that the Convention is an international instrument, the correct interpretation of which can be authoritatively expounded only by the Strasbourg court… The duty of national courts is to keep pace with the Strasbourg jurisprudence as it evolves over time: no more, but certainly no less."*

179. Recognising the IPT's reluctance to tackle the jurisdictional question without guidance from this Court, the Applicant's expressly reserved their jurisdiction position for consideration here, as noted by the IPT: "*It was, in the event, common ground that, subject to [counsel for the Applicants] 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 . . .*" (§50).

180. Finally, the UK Government raises a specific issue as to whether the Applicants exhausted their domestic remedies in respect of the issue of whether a system of prior independent authorisation is a requirement of a rights-compliant CNE regime. The Applicants did raise this issue before the IPT, as confirmed by the written submissions they filed in those proceedings: (i) the Applicants' skeleton argument refers on various occasions to the fact that section 7 CNE authorisations are "*conducted internally*" "*absence of any meaningful external or independent approval*", and (ii) paragraph 59a explicitly complains about the lack of any meaningful external or independent approval. Prior independent authorisation was expressly before the IPT and should have been considered by it.

181. The Applicants therefore did raise this point before the IPT. In any event, in *Fressoz and Roire v. France*, although the applicants at "*no stage, not even as an alternative submission*" complained, either expressly or in substance, of a breach of Article 10 of the Convention before the domestic courts, the Grand Chamber (§§38-39) unanimously dismissed the objection of the French Government that they had not raised their complaint in substance:

> *"the applicants relied on various provisions of the Freedom of the Press Act of 29 July 1881, which, so far as the applicants' activities are concerned, contains provisions equivalent to those of Article 10. In their pleadings in support of their appeal to that court, the applicants argued that their article had not contravened any provision of the Freedom of the Press Act and that, as a journalist, Mr Roire had simply been doing his "duty". In these circumstances, the Court holds that freedom of expression was in issue, if only implicitly, in the proceedings before the Court of Cassation and that the legal arguments made by the applicants' in that court included a complaint connected with Article 10 of the Convention."*

182. Similarly, in *Calleja v. Malta*, the Court found (admissibility decision):

> *"by raising the "reasonable time" issue before the competent domestic courts, the applicant invited them to examine the length of his trial and of his deprivation of liberty in the light of the Court's case – law…. By doing so, he complied with his obligation to make normal use of the available domestic remedies. Against this background, it is of little relevance that the applicant might not have explicitly drawn the attention of the Civil Court and of the Constitutional Court to the shortcomings which, according to him, had occurred during a specific stage of the proceedings."*

VIII. EFFECTIVE DOMESTIC REMEDY

183. The Court has held that, in order to be effective, "*a remedy must be capable of remedying directly the impugned state of affairs and must offer reasonable prospects of success*" (*Vučković and Others*, §§ 73-74 and *Sejdovic v. Italy* [GC], no. 56581/00, § 46, ECHR 2006-II).

184. At the time of the application, the IPT could not be considered to be an effective remedy. The Applicants therefore invite the Court to find a violation of Article 13 of the Convention for the following reasons:

184.1 The IPT as any UK court, does not have the power to quash a statute under human rights grounds. Nor does the IPT have power to issue a declaration that a statutory provision is incompatible with Convention Rights.

184.2 There was no judicial review available to the Applicants to challenge the decision of the IPT. Both the GCHQ and the IPT contended at the time that the findings of the IPT are not subject to judicial review;

184.3 There is no domestic remedy for a breach of Article 13 of the Convention. Article 13 is not included as a Scheduled enforceable right under the Human Rights Act 1998.

IX. APPLICANTS' REPLY TO THE COURT'S QUESTIONS

Question 1.

Can the applicants claim to be victims of a violation of the Convention, within the meaning of Article 34 in particular in light of *Roman Zakharov v. Russia [GC],* no. 47143/06, §§170-172, ECHR 2015?

Yes, for the reasons set out at paragraphs 151 to 158 above.

Question 2.

Have the applicants exhausted all effective domestic remedies, as required by Article 35 § 1 of the Convention?

In particular, in light of the "no determination" letter from the Investigatory Powers Tribunal did the applicants invoke before the national authorities at least in substance, the question of the jurisdiction of the United Kingdom?

Did the applicants invoke before the national authorities, at least in substance, the rights under Article 13 on which they now wish to rely before the Court?

Yes, for the reasons set out at paragraphs 173 to 182 above.

Question 3.

Did the facts of which the applicants complain in the present case occur within the jurisdiction of the United Kingdom?

Yes, for the reasons set out at paragraphs 159 to 172 above.

Question 4.

Has there been an interference with the applicants' right to respect for their private life, within the meaning of Article 8 § 1 of the Convention? If so, was that interference in accordance with the law and necessary in terms of Article 8 § 2?

There has been an interference, and it was neither in accordance with the law or necessary, for the reasons set out at paragraphs 50 to 136 above.

Question 5.

Has there been an interference with the applicants' freedom of expression, within the meaning of Article 10 § 1 of the Convention? If so, was that interference prescribed by law and necessary in terms of Article 10 § 2?

There has been an interference, and it was neither prescribed by law nor necessary, for the reasons set out at paragraphs 137 to 150 above.

Question 6.

Did the applicants have at their disposal an effective domestic remedy for their Convention complaints, as required by Article 13 of the Convention?

No, for the reasons set out at paragraphs 183 to 184 above.

BEN JAFFEY QC
TOM CLEAVER
Blackstone Chambers

CAROLINE WILSON PALOW
IOANNIS KOUVAKAS
Privacy International

MARK SCOTT
Bhatt Murphy