IN THE INVESTIGATORY POWERS TRIBUNAL **Case Nos. IPT 14/85, 120-126/CH**

B E T W E E N:

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

Claimants

-and-

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

Defendants

SKELETON ARGUMENT SERVED ON BEHALF OF THE CLAIMANTS

For hearing: Tuesday 1 December 2015

References in the form [AX/Y] are to Volume X, Tab Y of the Authorities Bundle.

References in the form [BX/Y/Z] are to Tab X, Page Y, Paragraph Z of the Open Bundle.

References beginning "CM" are to exhibits to the witness statements of Ciaran Martin.

References in the form [DX/Y/Z] are to Tab X, Page Y, Paragraph Z of the Open Documents.

A. Introduction

1. This case is about whether GCHQ has complied with domestic law and the ECHR when carrying out computer hacking[1] and deploying malware[2].

2. Until the open response was served, GCHQ refused to confirm or deny whether it had CNE capabilities, or had ever used them. This was a bizarre stance, since computer hacking tools are freely commercially available[3], and regularly used. As Professor Sommer put it "*if certain exploit tools can be deployed by 16 and 17 year olds to significant effect… then it would be very surprising if GCHQ were not able to call upon and use similar or better techniques*" [BB/69/17]. A more sensible approach is now taken; GCHQ has co-

[1] Known within the Agencies as CNE, Computer and Network Exploitation.
[2] A portmanteau word: malicious software, designed to intrude or have other effects unwanted by the owner or user of the computer.
[3] See [DA/99] ('Hacking Team', a commercial provider of CNE) and [69/15] (Report, Sommer).

operated in the production of a detailed schedule of avowals. With the possible exception of 'bulk CNE' (Issue 6(e))[4], the schedule has been agreed.

3. Further, until this claim was brought, GCHQ's CNE operations had been conducted without public knowledge of the applicable safeguards. The consequences have been predictable. When rules governing surveillance are not subject to public scrutiny or testing, public authorities tend to interpret their legal powers to maximise their ability to use intrusive measures, whilst failing to put in place adequate safeguards. As in other recent cases, litigation has spurred a belated attempt at compliance with the law.

CNE

4. Strong safeguards governing CNE are needed because, when deployed against an individual's computer or telephone, CNE can achieve results that are at least as intrusive as if the targeted individual were to have his house bugged, his home searched, his communications intercepted and a tracking device fitted to his person.

5. The intrusiveness of gaining access to a modern telephone was summarised by Chief Justice Roberts in *Riley v California* in the Supreme Court of the United States. The basic point is that "*a cell phone search would typically expose to the government far more than the most exhaustive search of a house…*" As Roberts CJ explained:

> "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video — that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier…"

6. Further, CNE techniques can be deployed against entire networks of communications infrastructure, giving access to numerous computers at once. The consequence is the ability to gain bulk access to the data of very large numbers of people.

[4] It is not understood why GCHQ is not willing to avow Bulk CNE, given that it told David Anderson QC it needed "the continued ability to acquire bulk data from a variety of sources, including through the use of new techniques, such as CNE" [CM1/7/258/10.40(a)]. Whether or not that means as a matter of strict construction that Bulk CNE is currently taking place, there can no longer be any serious prospect of any harm to national security from such confirmation being given, and the Respondents have made no effort to explain why they think there might be.

7. CNE is not a passive means of collecting intelligence, in contrast to interception. It requires active intrusion into a persons' computer, and often involves changing and altering the system to serve the purpose of the intruder. This has important consequences for the quality of the legal regime needed.

8. An intrusion into property that is not merely passive (such as a section 8(1) or 8(4) RIPA intercept) requires the strongest safeguards, not least because evidence obtained by CNE (and computers subject to CNE) is admissible in evidence, and forms the mainstay of many serious crime prosecutions. At its most serious, CNE can be destructive of people and property: for example, the 'Stuxnet' CNE operation which was aimed at disrupting nuclear centrifuges [BB/87/§72, DC/30].

9. Further, in order to carry out CNE, GCHQ must either seek or induce security holes in the systems that protect our computers, telephones and networks. Some of the more troubling elements of the Snowden disclosures are that the Five Eyes agencies have engaged in activities that weaken computer security for all (see Professor Anderson at [BB/54/§§49-77] and Mr King at [BB/22/§§70-116]. This has created a market in buying and selling computer vulnerabilities to nation states, and a strong incentive for nation states to weaken computer security to facilitate their access (see Professor Anderson at [BB/50/§§33-48] and Mr King at [BB/24/§§78-80]). Further, like any complex computer software, malware may have serious unintended effects. At the simplest level, users may be left vulnerable. Malware may spread beyond the intended targets.

Principles

10. CNE is thus a powerful and flexible technique, which carries greater risks to privacy and the security of the community than other forms of surveillance. In some limited cases, its covert use to gather information may be necessary and proportionate, subject to proper safeguards. Some CNE operations represent "… *a reasonable extension of how civilised societies have dealt with law enforcement intrusion into physical property for many years*" [Professor Anderson BB/47/19].

11. The issue is the presence of proper safeguards. As David Anderson QC notes, echoing the language of the ECtHR case law:

> "13.5 … in an age where trust depends on verification rather than reputation, trust by proxy is not enough. Hence the importance of clear law, fair procedures, rights compliance and transparency: not just fashionable buzz-words, but the necessary foundation for the trust between government and governed upon which the existence of coercive and intrusive powers depends in a modern democracy". [CM1/7/304]

In consequence:

> "13.18… if the acceptable use of vast state powers is to be guaranteed, it cannot simply be by reference to the probity of its servants, the ingenuity of its enemies or current technical limitations on what it can do. Firm limits must also be written into law: not merely safeguards, but red lines that may not be crossed" [CM1/7/307].

B. Issues

12. The parties have agreed preliminary issues of law as follows:

a) **Issue 1: Computer Misuse Act 1990 ("CMA 1990").** Before the CMA 1990 was amended with effect from 3 May 2015:

i. Was an act contrary to section 3 CMA 1990 (essentially, an unauthorised act in relation to a computer with the intention of, or recklessness as to, impairing its operation) capable of being rendered lawful by a statutory warrant?

ii. Would CNE activities of a Crown servant in the course of his employment, if committed in a foreign country or against assets or individuals located in a foreign country, have amounted to an offence under section 3 CMA 1990 as though the activities had been committed in England and against assets or individuals located in England?

b) **Issue 2: 'Thematic' warrants under section 5 Intelligence Services Act 1994 ("ISA 1994").** Does section 5 ISA 1994 permit the issue of a 'thematic' warrant authorising acts in respect of a class of property, or must such a warrant specifically identify the property to which it relates?

c) **Issue 3: Meaning of "property" in section 5 ISA 1994.** Does the power in section 5 ISA 1994 to issue a warrant authorising interference with "*property*" permit the issue of a warrant authorising interference with intangible legal rights, such as copyright or contractual rights?

d) **Issues 4 to 6: "*In accordance with law*"/"*prescribed by law*".** In view of the intrusiveness of CNE, has the regime governing CNE complied with Articles 8 and 10 of the European Convention on Human Rights at all times since 1 August 2009? In particular:

i) Is the regime sufficiently **foreseeable** in its operation?

ii) Are there sufficient safeguards to protect against **arbitrary conduct**?

iii) Is the regime **proportionate**?

iv) If domestic law permits the issue of 'class' or **'thematic' warrants**, does that regime comply with the above requirements or is specific authorisation necessary?

v) What **records** ought to be kept and with what degree of specificity as to the activity and the justification for it?

vi) What safeguards are necessary to prevent the obtaining, storing, analysis or use of **legally privileged material** and other sensitive **confidential documents**?

vii) What is the relevance of (i) the **various safeguards** relied upon by the Respondents, or (ii) the fact that until February 2015 it was **neither confirmed nor denied** that the Respondents carried out CNE activities at all?

C. Facts

13. Many of the relevant facts are now admitted. It is common ground that:

a) GCHQ undertakes CNE operations both within the UK and overseas.

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

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

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

e) GCHQ had five class authorisations under section 7 in 2014.

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

14. In addition:

a) **First**, the amount of information that can be derived through CNE techniques is large, and the nature of that information can be extremely sensitive. While interception of communications will result in the acquisition of information which an individual has chosen to communicate over a network, CNE may obtain information that a user has chosen not to communicate, for instance:

i) photos or videos stored on the device;

ii) documents;

iii) address book;

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

v) information collected through activation of the device's microphone or camera without the user's consent.

b) David Anderson QC refers to Snowden documents explaining several of these capabilities used by GCHQ: "*a programme called NOSEY SMURF which involved implanting malware to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, TRACKER SMURF which had the*

capability to provide the location of a target's smart phone with high-precision, and PARANOID SMURF which ensured malware remained hidden." [CM1/7/390/§15].

c) **Second**, CNE involves an active intrusion into a device or network. CNE techniques are not limited to the acquisition of information; it can be used to amend, add, modify or delete information, or to instruct the device to act or respond differently to commands.

d) **Third**, CNE allows for intrusion on a large scale. As well as specific devices, CNE can be used against networks of computers, or network infrastructure such as websites or internet service providers. For example, it appears that the Respondents carried out a CNE operation against a manufacturer of mobile phone SIM cards in order to allow the circumvention of its encryption and to enable "*harvesting… at scale*" [BB/18/§55].

e) Other examples include a CNE operation giving access to "*almost any user of the Internet*" in a targeted country [BB/14/§40] and systems designed for "*industrial scale exploitation*", appropriating the processing power of the target's computers to carry out searches and bulk analysis work [King BB/14/§42, 41/§138].

f) CNE can also be used against software, altering widely-used programs. For example, it appears that GCHQ has sought to modify or reverse-engineer commercially available software such as anti-virus software [DC/51/§4].

g) **Fourth,** CNE may leave users vulnerable to further damage:

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

ii) The process necessary to install the malware without alerting the user or his security software may result in or preserve security vulnerabilities that could be exploited by third parties.

iii) If the CNE takes place on a large scale – for instance in relation to network infrastructure, software, or common security protocols – it weakens security for all users, increasing the risk of exploitation by a third party. [Anderson BB/53/§§49-77].

D. Legislative framework

15. The legislative framework is set out in Annex 1 below.

E. Submissions

Issue 1a – section 10 of the CMA 1990

16. Many CNE operations will fall within section 3 CMA 1990. While a simple theft and use of login credentials would probably only engage section 1, section 3 could be engaged by:

a) the bypassing of security protections, particularly if those protections are weakened even temporarily as a result;

b) the use of the microphone or camera on a device in such a way as to drain the battery or slow the device down;

c) the processing or exfiltration of data, if to do so involves a significant use of system resources or bandwidth; or

d) the weakening of encryption or security protocols operated by the computer.

17. On a proper construction of section 10 CMA 1990, prior to amendment in May 2015:

a) a warrant (whether under ISA 1994 or PA 1997) could authorise CNE that would be a breach of section 1 CMA 1990 (i.e. hacking into a computer) but,

b) a warrant could not authorise CNE that would amount to the more serious offence of a breach of section 3 CMA 1990 (i.e. hacking into a computer and impairing its operation, including temporarily).

18. Parliament permitted law enforcement and intelligence agencies to gain access to computers to obtain information, but within strict limits. What Parliament did not authorise was CNE that impairs the operation of a computer.

19. Section 10 CMA 1990, prior to its amendment, provided: "*Section 1(1) above has effect without prejudice to the operation … in England and Wales of any enactment relating to powers of inspection, search or seizure*". The corollary is that section 3 does not have effect without prejudice to such enactments; Parliament placed limits on interference with computers. Section 5 ISA 1994 (and the equivalent provisions of PA 1997) are plainly enactments "*relating to powers of inspection, search or seizure*". They permit the electronic inspection and search of a computer.

20. Where a statute expressly provides for consequences only in one class of case, it follows that those consequences are excluded for other classes of case which could have been identified but were not.

21. There are sound reasons why Parliament set these limits:

a) First, the privacy intrusion involved in a section 1 offence more closely resembles a traditional search of premises or property. The section 3 offence is different: this type of hacking actually impairs the targeted device.

b) Secondly, the product of CNE is admissible in evidence. In that respect it is different from intercept evidence, which is inadmissible by section 17 RIPA 2000 and was inadmissible at the time of the passage of CMA 1990 under equivalent provisions of the Interception of Communications Act 1985. If state authorities are permitted to alter or impair the operation of a computer, the reliability and admissibility of such evidence will be called into question, as will the need to disclose a past CNE operation to the defence.

c) Thirdly, section 10 of CMA 1990 also applies to authorisations under PA 1997, as well as a section 5 ISA warrant. The above points apply with the same or greater force in relation to the police.

d) Finally, powers of search and seizure are to be construed narrowly against the public body seeking to search.

22. The same analysis also applies to authorisations under section 7 ISA.

23. The Snowden documents indicate that GCHQ's internal view was that section 10 of the CMA 1990 operated as set out above. A document prepared by a representative of GCHQ in September 2010 records a "*concern*" that a particular CNE technique which "*causes modification to computer data and will impact the reliability of the data*" "*may be illegal*", because "*The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material.*" [BA/9/§18(b)]

24. The Respondents' arguments as to why conduct constituting a s.3 offence may nevertheless be authorised lack merit:

a) It is irrelevant that ISA 1994 post-dates CMA 1990 (Open Response [BA/103/§146A(a))]. Section 5 ISA substantially re-enacts section 3 SSA 1989, which permitted the Secretary of State to issue a warrant "*authorising the taking of such action as is specified in the warrant in respect of any property so specified*". That provision pre-dated CMA 1990. When Parliament passed CMA 1990, it had already given the Security Service property interference powers, which were discussed in Parliament as permitting covert searches.

b) The ISA does not provide express authorisation for equipment interference. Section 5 is framed as a general power to authorise property interference. There are many types of property interference, or interference with electromagnetic emissions, that have nothing to do with a computer. For good reasons, the *lex specialis* in the CMA 1990 limits the scope of this broad power in the special case of interference with computers.

c) The Respondents argue at [BA/105/§146A(f)] that "*The interpretation contended for by the Claimants would lead to the absurd result that the authorisation mechanisms in the ISA could have no legal effect unless there was an express savings provision in each relevant piece of legislation*". That is incorrect. The point is not just that there was no savings provision in respect of the s.3 offence; it is that there was an express savings provision which could easily have applied to the s.3 offence but which instead applied only to the s.1 offence. That is a clear indication of Parliament's intention that there was to be no possibility of authorising a commission of the s.3 offence in pursuit of powers of inspection, search or seizure.

25. It is common ground that the Serious Crime Act 2015 has now altered the position. The amendments to section 10 are not retrospective, so the issue still arises for determination in respect of the period before 3 May 2015.

Issue 1b – Extraterritorial effect of CMA 1990

26. GCHQ now accept that CNE activities abroad will ordinarily breach CMA 1990 in the absence of authorisation ("*'class authorisations' signed by the Secretary of State under section 7 of the ISA… removes liability under the Computer Misuse Act 1990*") [DD/5].

27. However, if this remains in dispute:

    a) The jurisdictional provisions in CMA 1990 require "*at least one significant link with domestic jurisdiction*" (section 4(2)).

    b) There will be such a link if the accused was in "*the home country*" at the time when he did the act constituting the offence (section 5(2-3)).

    c) The "*home country*" is England and Wales, Scotland or Northern Ireland as appropriate (section 4(6)).

    d) GCHQ operates from sites in Cheltenham, Scarborough and Bude. Any CNE carried out from those locations over computers anywhere in the world will be subject to CMA 1990.

    e) Further, since the 2015 Act has come into force, any conduct abroad by a UK national which satisfies a dual criminality requirement will also be a "*significant link with domestic jurisdiction*" (section 5(1A)).

    f) In any event, section 31 of the Criminal Justice Act 1948 deems conduct carried out abroad by Crown servants acting or purporting to act in the course of their employment to be subject to English criminal law.

Issue 2 – 'Thematic' warrants under section 5 ISA

28. The issue of construction of section 5 ISA was accurately identified and properly brought to public attention by Sir Mark Waller in his 2014 Report, published on 25 June 2015[5]:

> "• Thematic Property Warrants
>
> I have expressed concerns about the use of what might be termed "thematic" property warrants issued under section 5 of ISA. ISA section 7 makes specific reference to thematic authorisations (what are called class authorisation) because it refers "to a particular act" or to "acts" undertaken in the course of an operation. However, section 5 is narrower referring to "property so specified".

[5] A keen reader of the ISC report (published on 12 March 2015) might have spotted a passing reference to thematic property warrants in footnote 34 of Chapter 3, three months prior to Sir Mark's report [CM14/581], but the Claimants did not.

During 2014 I have discussed with all the agencies and the warrantry units the use of section 5 in a way which seemed to me arguably too broad or "thematic". I have expressed my view that:

- section 5 does not expressly allow for a class of authorisation; and

- the words "property so specified" might be narrowly construed requiring the Secretary of State to consider a particular operation against a particular piece of property as opposed to property more generally described by reference for example to a described set of individuals. The agencies and the warrantry units argue that ISA refers to action and properties which "are specified" which they interpret to mean "described by specification". Under this interpretation they consider that the property does not necessarily need to be specifically identified in advance as long as what is stated in the warrant can properly be said to include the property that is the subject of the subsequent interference. They argue that sometimes time constraints are such that if they are to act to protect national security they need a warrant which "specifies" property by reference to a described set of persons, only being able to identify with precision an individual at a later moment". [CM1/16/849]

29. Sir Mark Waller was unwilling to go further than to note that the Agencies' interpretation was "*very arguable*". He recorded that one of the agencies had withdrawn a 'thematic' property warrant in light of his views [CM1/16/849]. Sir Mark is only content for a 'thematic' warrant to be issued "*where there is no intrusion into privacy*" (Martin 1 §71H).

30. A warrant power should be strictly construed. However, the Respondents have interpreted section 5 in an exorbitant manner. The Respondent claims that "*property so specified*" in a section 5 warrant can instead be "*specified… by description*", as opposed to by identification of the specific property [BA/107/146D(a)(v)]. That cannot be correct. It would permit a section 5 warrant to authorise property interference/CNE in the UK over:

a) "all mobile telephones in Birmingham";

b) "all computers used by suspected members of a drug gang";

c) "all copies of Microsoft Windows used by a person in the UK who is suspected of having travelled to Turkey in the last year"; or

d) "all software obtained by GCHQ".

31. The over-broad use of section 5 ISA is illustrated by some of the Snowden documents. On 22 June 2015, it was publicly disclosed that GCHQ had applied under section 5 ISA 1994 for a warrant authorising "*all continuing activities which involve interference with copyright or licensed software*" including "*modifying commercially available software to enable interception, decryption and other related tasks or "reverse engineering" software*" [DC/51-52/§1, 7].

32. The Agencies' expansive interpretation of section 5 ISA is wrong:

a) First, it would collapse the distinction between a section 5 'warrant' and a section 7 'authorisation'. Section 7 permits an authorisation of "*acts of a description*" or "*acts undertaken in the course of an operation so specified*" or acts affecting "*persons of a description so specified*". It therefore expressly permits the general authorisation of an entire operation, or a class of conduct. GCHQ appears to have made great use of that power, conducting all of its foreign CNE and other foreign activities pursuant to only five class authorisations [CM1/13/645/§234]. No similar wording permitting the authorisation of such wide classes or thematic operations is present in section 5.

b) Secondly, a 'thematic' warrant is in truth, a general warrant. A dislike of general warrants is a long-established principle of the common law. A 'thematic' warrant could only be available if clear words were used, thus overriding the limits long respected by the common law on the proper scope of state interference with property within the jurisdiction:

i) Under the principle of legality, Parliament is taken not to have interfered with fundamental rights, unless it uses clear words. See *R v SSHD, ex parte Simms* [2000] 2 AC 115 at 131 per Lord Hoffmann:

> "Parliamentary sovereignty means that Parliament can, if it chooses, legislate contrary to fundamental principles of human rights. The Human Rights Act 1998 will not detract from this power. The constraints upon its exercise by Parliament are ultimately political, not legal. But the principle of legality means that Parliament must squarely confront what it is doing and accept the political cost. Fundamental rights cannot be overridden by general or ambiguous words. This is because there is too great a risk that the full implications of their unqualified meaning may have passed unnoticed in the democratic process. In the absence of express language or necessary implication to the contrary, the courts therefore presume that even the most general words were intended to be subject to the basic rights of the individual. In this way the courts of the United Kingdom, though acknowledging the sovereignty of Parliament, apply principles of constitutionality little different from those which exist in countries where the power of the legislature is expressly limited by a constitutional document."

ii) A general warrant allows state officials, with no limits on time or place, to investigate a broad class of undesirable *conduct* (typically sedition in the 1700s, or a threat to national security now), rather than intrude on a specified *suspect* or *place*. In 1644, Coke condemned general warrants, as did Sir Matthew Hale in 1736. Hale explained that a "*general warrant to search in all suspected places is not good*" and "*not justifiable*" because it gave

such discretion to mere Crown servants "*to be in effect the judge*" (History of the Pleas of the Crown, p. 150).

iii) Most of the leading common law property interference cases concern general warrants. In all the cases, the threat to national security was urgent, and necessity may have required a warrant covering an operation rather than specified property. But the common law did not accede:

a) In *Huckle v Money* (1763) 2 Wilson 205, 95 ER 768 Lord Pratt CJ noted that: "*To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject*".

b) In *Wilkes v Wood* (1763) Lofft 1, 98 ER 489 the Lord Chief Justice said: "*The defendants claimed a right, under precedents, to force persons houses, break open escrutores, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject*." See also *Entick v Carrington* (1765) 2 Wilson 275.

iv) In the absence of clear and express words, Parliament has not departed from the traditional limits on search and seizure within the UK. There is nothing objectionable in a warrant that defines its target by reference to a specified person or premises. But legislation should not readily be construed as permitting a covert general warrant within the UK, in the absence of clear words, nor is such legislation necessary or proportionate.

c) Finally, if section 5 is ambiguous (which it is not), reference to Hansard assists:

i) Sections 5(1) and 5(2) ISA are based on sections 3(1) and 3(2) of the Security Service Act 1989, which permitted the Secretary of State to issue a warrant "*authorising the taking of such action as is specified in the warrant in respect of any property so specified*". In promoting the Security Service Bill, John Patten MP, the Minister of State for Home Affairs, explained to Parliament that a warrant issued under this power could only authorise "*action in respect of a named property, and both the action and the name of the property must be on the warrant*" (HC Deb 17 January 1989 vol 145, col 269, underlining added).

ii) Equally, the Claimants have found nothing in the Parliamentary debates leading to the passing of the ISA to suggest that Parliament contemplated that a section 5 warrant could authorise interference with a class of

property, specified by a broad description, as opposed to a specified item of property.

Issue 3 – Intangible property

33. The power in section 5 ISA permits interference with real property and personal property. It does not permit interference with a chose in action, such as intellectual property (or any other intangible right).[6]

34. The meaning of the word "*property*" depends on the context in which it is used.

a) In *R v Khan (Sultan Ashraf)* [1982] 1 WLR 1405, a deprivation order was made for the forfeiture of a convicted heroin dealer's house. The relevant power was contained in section 43(1) Powers of Criminal Courts Act 1973, which empowered a court to make an order in respect of "*property which was in his possession or under his control at the time of his apprehension"* which "*has been used for the purpose of committing, or facilitating the commission of, any offence"*. The Court of Appeal overturned the order on the grounds that the section was confined to "*personal property and not real property*". Per Dunn LJ at 1408: "*subsection (4), which makes the Police Property Act 1897 applicable, refers to property which is in the possession of the police by virtue of the section, thus confining it to personal property and not real property.*"

b) In *Welsh Development Agency v Export Finance Co Ltd* [1992] BCC 270, the Court of Appeal held that section 234 Insolvency Act 1986, in protecting an office-holder in certain circumstances where he "*seizes or disposes of any property which is not property of the company*", was limited to tangible property. Per Dillon LJ at 287: *"But subsec. (3) and (4) repeat the word 'seized' which was used in sec. 61 and is in its natural sense only applicable to tangible property and not to choses in action. Beyond that, se. 234(2) enables the court to give relief 'Where any person has in his possession or control any property, books, papers or records to which the company appears to be entitled'; that again appears at least primarily to be dealing with tangible property only. In my judgment, the references in sec. 234(3) and (4) to seizing property only apply to tangible property, and do not apply to choses in action."*

35. The provisions of ISA 1994 contain several clear indications that section 5 is concerned only with interference with physical property:

a) Section 5(3) and (3A) impose restrictions in relation to the issue of warrants in respect of "*property in the British Islands*".

b) Section 7(10) provides:

> "*Where-*
>
> *(a) A person is authorised by virtue of this section to do an act outside the British Islands in relation to property;*

[6] One of the Snowden documents indicates that "*the Intelligence Services Commissioner was consulted in 2005 on the applicability of a warrant in these circumstances* [in relation to intellectual property as embodied in copyright or licensing agreements] *and he was content that section 5 could be used to remove such liability*" [DC/54/§17].

(b) *The act is one which, in relation to property within the British Islands, is capable of being authorised by a warrant under section 5;*

(c) *A person authorised by virtue of this section to do that act outside the British Islands, does the act in relation to that property while it is within the British Islands, and*

(d) *The act is done in circumstances falling within subsection (11) and (12).*"

c) Section 7(11) provides: "*An act is done in circumstances falling within this subsection if it is done in relation to the property at a time when it is believed to be outside the British Islands.*"

d) Section 7(12) provides:

"*An act is done in circumstances falling within this subsection if it –*

(a) *Is done in relation to property which was mistakenly believed to be outside the British Islands either when the authorisation under this section was given or at a subsequent time or which has been brought within the British Islands since the giving of the authorisation; but*

(b) *Is done before the end of the fifth working day after the day on which the presence of the property in the British Islands first becomes known.*"

e) Section 7(13) and (14) make further provision in relation to the relevant dates for the purposes of section 7(12), and refer to "*the belief that the property was outside the British Islands*", the property being "*within those Islands*", and the property being "*brought within the British Islands*".

36. These provisions are inconsistent with section 5 covering intangible property, such as a chose in action or a copyright. How can a copyright or right of action be "*brought within the British Islands*"?

Copyright

37. A particular issue arises in respect of interference with copyright, in view of the rights conferred by the Copyright Directive (Directive 2001/29).

38. Article 2 of Directive 2001/29 provides: "*Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part (a) for authors, of their works …*".

39. National law must so far as possible be construed in accordance with that obligation, in accordance with the principle in Case C-106/98 *Marleasing*: *ITV Broadcasting Ltd v TVCatchup Ltd* [2011] EWHC 2977 (Pat) at [35].

40. Article 5 of the Directive sets out an exhaustive list of possible exceptions or limitations to the Article 2 right. The only relevant exception is Article 5.3(e), which enables Member States to provide for an exception for "*use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings*". Further, Article 5.5 provides that such exceptions "*shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.*"

41. Accordingly, any interference with copyright by the authorities of a Member State must satisfy the following requirements of EU law:

    a) It must be clearly provided for in law, satisfying "*the need for legal certainty for authors with regard to the protection of their works*": C-14/10 Painer v Axel Springer at [100-110];

    b) It must not conflict with a normal exploitation of the work and must not unreasonably prejudice the legitimate interests of the rightholder: Article 5.5; and,

    c) It must comply with the general EU law of proportionality, satisfying the "*relatively intensive and thorough*" standard of review which applies in respect of interferences with copyright: *BASCA v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin) at [135].

42. If the Respondents have been operating section 5 ISA 1994 so as to purport to justify interference with copyright for the purpose of reverse-engineering software, that is non-compliant with the first two requirements (and its compliance with the third is a question of fact). The reverse-engineering of software – presumably with a view to developing malware – obviously conflicts with the normal exploitation of those works.

43. In their pleaded Response, the Respondents say "*the relevance of Directive 2001/29 is not understood*" because "*the relevant law of copyright is the domestic law of England and Wales*" [BA/107/146F]. The Directive is relevant to the effect of domestic law for two reasons:

    a) First, because of the obligation recognised in *Marleasing* to interpret domestic legislation as far as possible in accordance with an EU directive. It is a heavy obligation: as Arden LJ held in *HMRC v IDT Card Services (Ireland) Ltd* [2006] EWCA Civ 29 at [82], in view of an inconsistent provision of EU law "*the English courts can adopt a construction [of domestic law] which is not the natural one.*" Even if Section 5 ISA were ambiguous (which it is not), *Marleasing* interpretation would require that it be construed in such a way as to preclude interference with copyright contrary to the Directive.

    b) Second, because a Court is bound to give direct effect to "*unconditional and sufficiently precise*" provisions of a directive as against a public authority even if to do so would be *contrary* to domestic law: C-41/74 *Van Duyn v Home Office* at

[11]. Where rightholders are concerned, Article 2 of Directive 2001/29 is such a provision, and must therefore be given effect.[7]

Issue 4 – Prescribed by law

Foreseeability

44. By section 6 of the Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with one of the rights set out in Schedule 1 to the Act, which incorporates the European Convention on Human Rights ("ECHR") [A1/6].

45. Article 8 of the Convention provides:

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

46. There are therefore four questions:

a) Is the Article 8(1) right engaged?

b) Does the interference comply with the requirement of legal certainty imposed by the relevant Article?

c) Is the interference in pursuit of a legitimate aim?

d) Is the interference proportionate to the goal that is sought to be achieved (in the case of Article 8, "*necessary in a democratic society*…")? [A1/6]

Engagement of rights

47. Article 8 of the ECHR is clearly engaged in the present case.

Legal certainty

[7] The Response also says, at [BA/107/146F]: "*It is not contended that the United Kingdom has failed to implement Directive 2001/29 in domestic law.*" It is unclear what is meant by that submission. As is clearly pleaded at [BA/22/41E], the Directive imposes certain requirements on a Member State. If those requirements have not been met – for instance because a public authority has interfered with copyright in a manner which does not meet them, or because the law is insufficiently clear as to whether there could be such an interference – then it follows the United Kingdom will have failed to implement Directive 2001/29 properly. In those circumstances the Court will have to give effect to it, either by reading down the domestic provisions, or giving effect to the Directive directly against a public authority in any case where a person's directly effective rights are engaged.

48. Any interference with Article 8 must be "*in accordance with the law*" (see Article 8(2) [A1/6]). This requires more than merely that the interference be lawful as a matter of English law: it must also be "*compatible with the rule of law*" (*Gillan v United Kingdom* (2010) 50 EHRR 45 at §76). There must be "*a measure of legal protection against arbitrary interferences by public authorities*", and public rules must indicate "*with sufficient clarity*" the scope of any discretion conferred and the manner of its exercise: *Gillan* at §77.

49. There are therefore three sub-requirements:

a) the conduct must comply with domestic law (legality);

b) the public rules must be sufficiently clear and describe the scope of any discretion and the manner of its exercise (foreseeability); and

c) there must be adequate legal protection against arbitrary interference with privacy (arbitrariness).

50. Numerous cases have addressed these requirements in the context of secret surveillance and information gathering:

a) In *Malone v United Kingdom* (1985) 7 EHRR 14 [A2/42], the Court held that the legal regime governing interception of communications "*must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*" §67. It must be clear "*what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive" and the law must indicate "with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities*" §79.

b) In *Association for European Integration and Human Rights v Bulgaria* (62540/00, 28 June 2007) [A2/30], the Court held at §75:

> "In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for us is continually becoming more sophisticated …"

c) These requirements apply not only to the collection of material, but also to its treatment after it has been obtained, including the "*procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material*" (*Liberty v UK* (2009) 48 EHRR 1 at §69).

d) In *Weber & Saravia v Germany* (2008) 46 EHRR SE5 [A2/49] the ECHR held at §§93-94:

> "The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the

> conditions on which public authorities are empowered to resort to any such measures … Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

e) In *Weber* the Court at §95 set out minimum safeguards (with numbers and spacing added for clarity):

> "In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power:
>
> > [1] the nature of the offences which may give rise to an interception order;
> >
> > [2] a definition of the categories of people liable to have their telephones tapped;
> >
> > [3] a limit on the duration of telephone tapping;
> >
> > [4] the procedure to be followed for examining, using and storing the data obtained;
> >
> > [5] the precautions to be taken when communicating the data to other parties; and
> >
> > [6] the circumstances in which recordings may or must be erased or the tapes destroyed."

f) *Weber* was an interception case, but the principles in *Weber* have wider application to cases involving surveillance of all kinds. The touchstone is whether the degree of interference with privacy is comparable to that involved in interception of communication. See *RE v UK* at §130 ("*the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference*" [A2/44]. Cf. *Uzun v Germany* [A2/48] where the full *Weber* criteria were not applied because the case only involved collection of the location of a vehicle, generally on public roads or visible from the street. For the reasons set out above, CNE is at least as intrusive as traditional intercept, often far more so.

51. Applying these principles, the ECtHR has repeatedly held that the intercept and surveillance practices of the UK did not include sufficient public and binding safeguards and did not comply with the "*in accordance with the law*" requirement. See, for example, *Malone* [A2/42], *Liberty v UK* [A2/41], *Khan v UK* [A2/37] and *RE v UK* [A2/44].

Similarly, see *Liberty/Privacy* on foreseeability of 8(4) interception and *Belhaj* in the IPT (by concession) [A2/22-23 and A1/16].

52. This issue is not one in which the Court gives any margin of discretion to the state. See the judgment of Lord Reed in *R (T) v Chief Constable of Greater Manchester* [2014] 3 WLR 96 at §114:

> "Whether a system provides adequate safeguards against arbitrary treatment, and is therefore "in accordance with the law" within the meaning of the Convention, is not a question of proportionality, and is therefore not a matter in relation to which the court allows national authorities a margin of appreciation."

Domestic law

53. For the reasons set out above, GCHQ has not correctly understood or applied domestic law governing CNE. There is therefore a breach of the first limb of the "*in accordance with the law*" requirement.

Prior to the Open Response/First Draft EI Code

54. The *Privacy International* claim was issued on 13 May 2014. The Open Response was served on 6 February 2015, at the same time as the publication of the First Draft EI Code. Prior to the service of the Open Response, nothing at all was known about the rules or safeguards governing CNE. The *Weber* criteria were not satisfied:

a) The Property Code was the only public information about the use of CNE (even assuming it could be deduced that property interference included CNE, which is far from obvious).

b) The Property Code is very brief as applied to section 5 authorisations and does not engage with *Weber* requirements 4, 5 or 6.

c) The position in relation to section 7 ISA is even worse. There was no Code of Practice governing the use of section 7 (nor even a power to issue one). Section 7 was an unexplained bare power, even though section 7 might often affect people in the United Kingdom. This may occur in three ways:

   i) First, where a mistake is made as to location, or in the 5-day grace period under section 7(11) ISA.

   ii) Secondly, where a person in the UK stores (as we all do) their data outside the UK. See Martin 1 at [BB/133/§44].

   iii) Thirdly, foreign CNE conduct will often affect people in the UK. For example, if a CNE operation steals the keys for all SIM cards produced by a foreign manufacturer (such as Gemalto), many of those cards will end up in the UK and be used by UK persons.

The availability of a warrant that simply cancels any unlawfulness is self-evidently not an adequate safeguard against arbitrary conduct.

55. This absence of proper public procedures was not for good reasons of national security – the use of CNE was admitted once the claim had been brought, and was formally avowed in the ISC and Anderson Reports. The position is worse than the pre-IOCA 1985 days of intercept considered by the ECtHR in *Malone*. A useful comparator is *Liberty v UK* where there was no Code of Practice governing bulk interception under IOCA 1985, nor any public safeguards or limits on a wide statutory power. The subsequent introduction of the RIPA Interception Code of Practice demonstrated the inadequacy of what went before [A2/41].

56. The failing is not simply technical. As David Anderson QC puts it:

> "Obscure laws – and there are few more impenetrable than RIPA and its satellites – corrode democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean. Thus:
>
> > (a)… ISA 1994 ss 5 and 7… are so baldly stated as to tell the citizen little about how they are liable to be used" [CM1/7/310/§13.31].

After the Open Response/First and Second Drafts of the EI Code

57. Publication of the draft EI Code does not cure the problems:

a) First, the specific failings in relation to the Draft EI Codes are set out below under issue 5.

b) Secondly, the EI Code is only in draft, not yet approved.

Article 10 ECHR

58. The same analysis of the issues applies under Article 10 ECHR.

Issue 5

59. *(a) Specific and individual or class warrants*:

a) The over-broad approach to the use of section 5 ISA thematic warrants has been considered above. The dangers of general warrants are present more strongly in the case of section 7 ISA class authorisations. There were only five such authorisations in place in 2014 which covered all of the agencies' CNE activities abroad. All authorisation is then conducted internally. This absence of any meaningful external or independent approval for highly intrusive conduct is a significant failing in the regime. Several additional failures are set out below.

b) First, under the draft EI Code there is inadequate protection for people in the British Islands whose data is obtained by CNE abroad. For example, assume a Londoner's smartphone stores photographs on a computer server in the Republic of Ireland. GCHQ wishes to look at the photos. There are three sets of statutory powers it could use:

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

ii) RIPA could be used to obtain the photos. Interception under RIPA includes any time when information is stored after being transmitted (section 2(7) [A10]).

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

b) Assuming that a bulk warrant under section 8(4) of RIPA is used, the person has the equivalent safeguard that GCHQ would require a section 16(3) certification, which is for practical purposes identical to a Secretary of State warrant.

iii) Section 7 ISA could be used to obtain the photos under GCHQ's class authorisation. No Secretary of State warrant is required, nor is there any equivalent certification procedure. GCHQ can authorise the obtaining of the photos internally. Important safeguards that are a crucial part of maintaining the lawfulness of the RIPA interception regime are absent.

iv) In this scenario, the Draft EI Codes do not provide any substantial safeguard:

> "If a member of SIS or GCHQ wishes to interfere with equipment located overseas but the subject of the operation is known to be in the British Islands, consideration should be given as to whether a section 8(1) interception warrant or a section 16(3) certification (in relation to one or more extant section 8(4) warrants) under the 2000 Act should be obtained in advance of commencing the operation authorised under section 7."

David Anderson QC rightly observes that the Code "*does not elaborate on what factors should be taken into account in the course of that consideration*" [CM7/161/6.33]. In contrast, other provisions of the Draft EI Codes are phrased in terms of "*should*" or "*must*".

c) The important safeguard in RIPA of a Secretary of State warrant is thus liable to be circumvented by a general power in section 7. The protection given to the citizen is greatly reduced.

d) Secondly, there are no procedures in the Draft EI Code requiring the use of filtering techniques where bulk CNE is carried out[8] (see Issue 6(e) – "*the use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest*"). The Commissioner has encouraged the use of such filters when considering data collected under

[8] The Claimants reserve their position as to the IPT's approach of the use of bulk collection in *Liberty/Privacy*.

section 7 ("*I stressed to* [GCHQ] *the importance I place on filters which help avoid any unnecessary intrusion*" [CM16/856]).

e) However, the Commissioner's exhortation is not backed by any obligation, either in statute or a Code of Practice. Again, the contrast with RIPA is striking:

i) Under section 16(1) RIPA, inspection of bulk material is limited by a certificate. This is the key safeguard in respect of bulk collection. In *Liberty/Privacy* the Tribunal accepted Liberty's submission that section 16 was needed to do the "*heavy lifting*" of protecting privacy if a large volume of data was being collected. The Tribunal held "*we do not accept that it is, simply, as Mr Eadie put it in Reply submissions, "procedural""* [A2/22/§103].

ii) The certificate is supplemented by detailed provisions in the Interception Code of Practice requiring the use of automated filtering systems using an effective selection methodology, the giving of reasons before making any selection etc. These safeguards are essential to the lawfulness of such bulk techniques. They are not required in respect of material collected in bulk under section 7 ISA, either by the legislation, or the applicable Code of Practice (Section 7 of the Interception of Communications Code of Practice).

f) Finally, even where a section 5 ISA warrant is obtained, it could be used to target computer networks, servers and other devices used by individuals or organisations that are not of any intelligence interest in and of themselves.

60. (b) *Record keeping* – GCHQ contend that they keep better records than the other Agencies. This may be right (see Commissioner's 2014 report [CM1/17/856]). However, the records that are required to be kept by the draft EI Code are at the stage of authorising the CNE operation, not the documentation of the searches that take place of the data obtained.

61. (c) *Legal Professional Privilege* – The regime prior to the publication of the Draft EI Codes was not in accordance with the law for the same reasons as in *Belhaj*:

a) GCHQ conceded in *Belhaj* that its procedures in relation to intercept of privileged material were not lawful.

b) Although the Property Code was drafted in better terms than the Interception Code (see [CM1/16/777/§4.26]), that was not reflected in GCHQ's internal policies. The concession in *Belhaj* was rightly made:

i) The definition of privilege in GCHQ's procedures is inadequate – it ignores litigation privilege. See [CM2-5/§14-16].

ii) The guidance does not recognise that 'events', metadata and communications data may be privileged (as to which see below). See [CM2-5/§5].

iii) GCHQ had no internal information barrier policies to deal with cases in which it was a party to actual or potential litigation. The information barrier procedures applied by GCHQ were inadequate, leading to a determination against GCHQ in respect of Mr Al-Saadi.

62. The regime after the publication of the draft EI Codes remains inadequate:

a) The First Draft EI Code proposed a number of welcome improvements:

i) Privilege is properly defined, by reference to section 98 of the PA 1997 [CM1/15/714/§3.2]

ii) Proper information barriers "*must*" be put in place to ensure that lawyers and policy officials do not see privileged materials, with provision for applying to the Court in cases of doubt [CM1/15/716/§3.17].

b) The Second Draft EI Code proposed certain further improvements:

i) Communications between lawyer and client and between a lawyer and another person for the purposes of litigation are presumed to be privileged unless the contrary is established (para. 3.4).

ii) Sensibly, given the past tendency of the Agencies to introduce internal glosses on necessary and proper information barriers, the Code expressly provides that "*For the avoidance of doubt, the guidance in paragraphs 3.1 to 3.18 takes precedence over any contrary content of an agency's internal advice or guidance*".

c) But the Second Draft EI Code also worsens the language by changing the mandatory "*must*" to a discretionary "*should*" (e.g. para. 3.17). The protection of privilege ought to be mandatory.

d) Further, both Draft EI Codes are silent on whether 'events' information or metadata can be privileged. However, it is clear from GCHQ's current internal procedures at [CM2-9] that GCHQ continues to consider that privilege does not attach to the fact of a communication between lawyer and client or witness or expert:

> "Reporters should also remember that <u>the additional sensitivity attaches to the content of the communications, not to the fact of communication having taken place. Metadata only reports featuring lawyers do not require mandatory checking by the relevant team</u>."

e) This approach is wrong in law. Metadata will often be subject to legal professional privilege without sight of the content. For example, the fact of a communication between a lawyer and a potential witness is itself privileged information and will be disclosed by the fact of the communication alone. Whether a lawyer or client has spoken to a particular witness or potential expert is often very sensitive privileged information, deserving of strict protection. The dates, times, place and parties to legally privileged communications are

information that is as privileged as the substance of the communication. See *Passmore on Privilege, 3rd Ed* para. 9-007 – 9-008. Just as journalists are entitled to protect their sources, a litigant (or criminal defendant) is entitled to consult an expert or speak to a witness without the opposing party knowing that fact. In such cases, GCHQ's policies currently apply no information barriers, nor any restriction on the wider distribution of such information to partner agencies or others in government. For a detailed analysis of the legal errors in this approach, the Claimants rely on the submissions of the Law Society in the *DRIPA* litigation, a copy of which is attached to this skeleton.

f) Even today, GCHQ has not formally introduced the proper information barrier procedures required by *Belhaj*. The procedures are still "*awaiting formal approval by the relevant GCHQ senior official*" (Martin 2, §18). An *ad hoc* Chinese wall policy is not sufficient in law. See *Prince Jefri Bolkiah v KPMG* [1999] 2 AC 222 Lord Millett at p. 239:

> "… In my opinion an effective Chinese wall needs to be an established part of the organisational structure of the firm, not created ad hoc..."

63. (d) *Previous NCND stance* – The Claimants' submissions are set out above.

64. (e) *Property Interference Code* – The Claimants' submissions are set out above. In short, the Property Interference Code does not even recognise the existence of CNE, still less put in place appropriate procedures to deal with intrusive CNE operations.

65. (f) *Draft EI Codes* – The Claimants' submissions are set out above.

66. (g) *Commissioner's oversight* – The Commissioner's oversight has in the past been ineffective. For example:

a) The Commissioners all failed to identify the defects in the Agencies' procedures that led to the concession in *Belhaj*.

b) No inspection had ever been made of the "*Additions layer*" which is "*the layer at which individual targets are usually described*" under section 7 ISA until April 2015 [BB/141/§71I]. Mr Martin's explanation of the Commissioner's recommendations following the inspection is Delphic ("*The Commissioner recommended changes be made to ensure that each element is dealt with explicitly and at the earliest opportunity*"). A comprehensible explanation ought to be disclosed.

c) The Commissioner had not identified that "*until recent years, renewal instruments for section 5 warrants had contained the minimum wording stipulated by ISA section 6*" [BB/141/§71E]. This appears to mean that a renewal instrument simply said words to the effect of 'I renew warrant [number] for 6 months.' The Commissioner asked GCHQ to add a reminder to the Secretary of State of the statutory test.

67. (h) *Role of the Tribunal* – The Claimants reserve their position as to whether it is proper for the Tribunal to consider any closed material for the purpose of determining the

preliminary issues. To the extent that any EU law issues arise, the Claimants note that there is no domestic right of appeal against a decision of the Tribunal.

Is the regime proportionate?

68. For the reasons set out above, the regime governing CNE was not and remains disproportionate. Given the high potential level of intrusiveness, including over large numbers of innocent persons, there are inadequate safeguards and limitations.

F. Conclusion

69. The Tribunal is invited to answer the Preliminary Issues as set out above.

BEN JAFFEY

TOM CLEAVER

Blackstone Chambers

BHATT MURPHY

25 November 2015

Annex 1 – Legislative Framework

Computer Misuse Act 1990

1. The CMA 1990 provides for specific (and often extra-territorial) criminal liability for CNE. There are two key offences:

   a) Section 1 provides an offence of unauthorised access to a computer.

   b) Section 3 provides for the more serious offence of impairing the operation of a computer, even temporarily.

2. The Section 1 offence carries a maximum sentence of two years' imprisonment:

   "(1) A person is guilty of an offence if—

   (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

   (b) the access he intends to secure, or to enable to be secured, is unauthorised; and

   (c) he knows at the time when he causes the computer to perform the function that that is the case".

3. The Section 3 offence carries a maximum sentence of ten years' imprisonment:

   "(1) A person is guilty of an offence if–

   (a) he does any unauthorised act in relation to a computer;

   (b) at the time when he does the act he knows that it is unauthorised; and

   (c) either subsection (2) or subsection (3) below applies.

   (2) This subsection applies if the person intends by doing the act–

   (a) to impair the operation of any computer;

   (b) to prevent or hinder access to any program or data held in any computer;

   (c) to impair the operation of any such program or the reliability of any such data; or

   (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to–

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section …

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily."

4. Sections 4 and 5 make various provisions in relation to the territorial scope of both offences.

a) Section 4(1) provides that, subject to the remainder of that section, it is immaterial "*whether any act or event proof of which is required for conviction of the offence occurred in the home country* [England and Wales, Scotland or Northern Ireland as appropriate] *concerned*".

b) Section 4(2) requires "*at least one significant link with domestic jurisdiction*".

c) Section 5(3) provides that there is such a link in relation to the section 3 offence if "*the accused was in the home country concerned at the time when he did the unauthorised act (or caused it to be done)*" or "*the unauthorised act was done in relation to a computer in the home country concerned*".

d) Section 5(2) makes similar provision in relation to the section 1 offence.

5. Section 31 CJA 1948 provides:

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

6. Section 10 CMA 1990 contains saving provisions:

a) Prior to 3 May 2015, section 10 provided: "*Section 1(1) above has effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure …*"

b) Following its amendment by the Serious Crime Act 2015, s.10 now provides: "*Sections 1 to 3A have effect without prejudice to the operation (a) in England and Wales of any enactment relating to powers of inspection, search or seizure or of any other enactment by virtue of which the conduct in question is authorised or required*" (amendments underlined).

7. The 'Explanatory Notes' to the Serious Crime Act 2015 did not flag any significant change in relation to section 10. Instead, they said at paragraph 139:

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

8. The chronology of the change to the legislation was as follows:

a) On 13 May 2014, Privacy International issued these proceedings, squarely raising the issue of the interaction between section 3 and section 10 CMA 1990 at paragraph 37 [A/17].

b) On 5 June 2014, the Serious Crime Bill had its First Reading in the House of Lords. It contained, at clause 40, the amendments which were ultimately implemented as set out above.

c) On 6 February 2015, the Respondents served an Open Response summarising the effect of sections 1 and 3 separately but not pleading to the issue identified in the Statement of Grounds. [A/68-69].

d) On 3 March 2015, the SCA 2015 received Royal Assent.

e) On 3 May 2015, the amendments made to the CMA 1990 by the SCA 2015 came into force.

Intelligence Services Act 1994

9. Section 3(1)(a) ISA provides that GCHQ's functions include "to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material". Section 3(2) ISA stipulates that

these functions are exercisable only in the interests of national security, the economic well-being of the United Kingdom, or the prevention or detection of serious crime.

10. Section 4(2)(a) ISA provides that one of the duties of the Director of GCHQ is to secure that *"no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings"*.

11. Section 5 ISA provides:

> "(1) No entry on or interference with property or with wireless telegraphy shall be unlawful if it is authorised by a warrant issued by the Secretary of State under this section.
>
> (2) The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHQ, issue a warrant under this section authorising the taking, subject to subsection (3) below, of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified if the Secretary of State—
>
> > (a) thinks it necessary for the action to be taken for the purpose of assisting, as the case may be,—
> >
> > …
> >
> > (iii) GCHQ in carrying out any function which falls within section 3(1)(a) above; and
>
> (b) is satisfied that the taking of the action is proportionate to what the action seeks to achieve;
>
> (c) is satisfied that satisfactory arrangements are in force under …section 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained under the warrant will be subject to those arrangements."

12. Section 5(3) ISA provides that a warrant authorising interference with property within the British Islands can only be issued to GCHQ for its functions in respect of national security or the economic well-being of the UK. Within the UK, the Security Service handles the prevention and detection of serious crime, although GCHQ may in practice act on its behalf in actually carrying out interference.

13. In relation to section 5 warrants, section 6 ISA provides:

a) at section 6(1), that warrants may only be issued under the hand of the Secretary of State or, in urgent cases, certain other officials;

b) at section 6(2), that warrants issued by the Secretary of State expire after six months unless renewed;

c) at section 6(3), that the Secretary of State may renew a warrant for 6 months at any time;

d) at section 6(3), that the Secretary of State shall cancel a warrant *"if he is satisfied that the action authorised by it is no longer necessary"* (Section 6(4)).

14. In contrast, section 7 ISA provides:

> "(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section.
>
> (2) In subsection (1) above "liable in the United Kingdom" means liable under the criminal or civil law of any part of the United Kingdom.
>
> (3) The Secretary of State shall not give an authorisation under this section unless he is satisfied—
>
> > (a) that any acts which may be done in reliance on the authorisation or, as the case may be, the operation in the course of which the acts may be done will be necessary for the proper discharge of a function of the Intelligence Service or GCHQ; and
> >
> > (b) that there are satisfactory arrangements in force to secure—
> >
> > > (i) that nothing will be done in reliance on the authorisation beyond what is necessary for the proper discharge of a function of the Intelligence Service or GCHQ ; and
> > >
> > > (ii) that, in so far as any acts may be done in reliance on the authorisation, their nature and likely consequences will be reasonable, having regard to the purposes for which they are carried out; and
> >
> > (c) that there are satisfactory arrangements in force under section 2(2)(a) or 4(2)(a) above with respect to the disclosure of information obtained by virtue of this section and that any information obtained by virtue of anything done in reliance on the authorisation will be subject to those arrangements.
>
> (4) Without prejudice to the generality of the power of the Secretary of State to give an authorisation under this section, such an authorisation—
>
> > (a) may relate to a particular act or acts, to acts of a description specified in the authorisation or to acts undertaken in the course of an operation so specified;
> >
> > (b) may be limited to a particular person or persons of a description so specified; and

(c) may be subject to conditions so specified.

…

(9) For the purposes of this section the reference in subsection (1) to an act done outside the British Islands includes a reference to any act which—

(a) is done in the British Islands; but

(b) is or is intended to be done in relation to apparatus that is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus."

Section 7 also sets out provisions for the issue, renewal and cancellation of warrants, which broadly mirror those for warrants issued under section 5.

15. The power under section 7 to authorise acts outside the British Islands is much broader than the power in section 5. In particular:

a) Section 7 is not limited to actions in respect of property or wireless telegraphy. It could be (and is) used to authorise a variety of other activities, including the recruitment of agents and the payment of bribes or inducements.

b) Section 7(4) permits the authorisation of acts by reference to a description of people or a class of operations, rather than merely in relation to *"specified"* property.

Police Act 1997

16. The ISA powers are very similar to the property interference powers available to the police under Part III of the Police Act 1997. The power to authorise interference is exercisable by senior police officers in their area, or more widely in certain cases:

a) section 93(1)(a) provides: "*Where subsection (2) applies, an authorising officer may authorise … the taking of such action, in respect of such property in the relevant area, as he may specify …*";

b) section 93(2) establishes two cumulative criteria: first, that the authorising officer believes "*that it is necessary for the action specified to be taken for the purpose of preventing or detecting serious crime*", and second, that the authorising officer believes "*that the taking of the action is proportionate to what the action seeks to achieve*"; and

c) the Act also provides for authorisations to be reviewed by independent judicial Commissioners appointed under section 91, and makes specific provision in relation to the protection of legally privileged information: sections 97 and 98.

Property Interference Code of Practice

17. The Home Office has published a "Covert Surveillance and Property Interference Code of Practice" pursuant to section 71 RIPA [CM15/734, A1/10]. It has been referred to by the Respondents as the "Property Code", and that definition is adopted for convenience, although in fact it is concerned overwhelmingly with covert surveillance.

18. The version currently in force was published in December 2014, but, as the Respondents note "*in terms of property interference there is no material difference between the 2010 and the 2014 versions of the Code*": [BA/95/§101].

19. Importantly:

    a) The Property Code is only relevant to warrants issued under section 5 ISA 1994 [CM1/15/738/1.3]

    b) The Property Code does not apply to warrants issued under section 7 ISA 1994.

    c) The Secretary of State does not, even today, have statutory power to issue a Code in relation to section 7 ISA 1994.

20. The key provisions of the Property Code relating to property interference under section 5 ISA 1994 are:

    a) Paragraph 7.18, which sets out information which should be provided in support of an application (including "*sufficient information to identify the property which the entry or interference with will affect* [sic]");

    b) Paragraph 7.19, which provides that in urgent cases the information may be submitted orally;

    c) Paragraphs 7.36 to 7.42, which concern warrants for property interference by the intelligence services, and essentially state that the same information should be provided; and,

    d) Section 8, which states that specified information pertaining to all authorisations "*shall be centrally retrievable within each public authority for a period of at least three years from the ending of each authorisation*".

Draft Equipment Interference Code of Practice

21. The Home Office also published a draft Equipment Interference Code of Practice ("First Draft EI Code") on 6 February 2015. On the same day, the Respondents served their Open Response in these proceedings. The Respondents do not suggest this timing is a coincidence.

22. On 4 November 2015, the Respondents published a revised draft Equipment Interference Code ("Second Draft EI Code"). The Claimants have prepared a tracked changes version, which illustrates the significant changes between drafts.

23. The Second Draft EI Code remains a draft, and has not been brought into force. The most significant paragraphs of the Draft EI Code are as follows [CM1/14/708]:

a) Paragraph 1.2: The EI Code takes precedence over the Property Code.

b) Paragraph 1.4: Although there is no power to make a Code about Section 7, as a matter of policy, the First Draft EI Code requires that it "must" be applied to equipment interference under section 7 (the wording in the Second Draft EI Code has reduced the mandatory "must" to a discretionary "should").

c) Paragraph 1.9 states: "*Equipment interference is conducted in accordance with the statutory functions of each Intelligence Service*", avowing the practice of CNE.

d) Footnote 1 defines "Equipment" very broadly. It "*may include, but is not limited to, computers, servers, routers, laptops, mobile phones and other devices*".

e) Section 3 contains purported safeguards for legally privileged and confidential information.

f) Section 4 sets out the procedures for authorising equipment interference under section 5 ISA 1994.

i) Paragraph 4.6 sets out the information which an application for a s.5 warrant must contain, including "*the identity or identities, where known, of those who possess or use the equipment that is to be subject to the interference*" and "*sufficient information to identify the equipment which will be affected by the interference*".

ii) Further, the First Draft EI Code requires application to describe "*any action which may be necessary to install, modify or remove software on the equipment*". The Second Draft EI Code added the words "*including an assessment of the consequences (if any) of those actions*".

g) Paragraph 6.3 provides that information obtained through equipment interference may be used as evidence in criminal proceedings.

h) Section 7 sets out the procedures for authorising equipment interference under section 7 ISA 1994.

i) Paragraph 7.6 states: "*An authorisation under section 7 may be specific to a particular operation or user, or may relate to a broader class of operations.*"

ii) Paragraph 7.11 reiterates "*An authorisation under section 7 may relate to a broad class of operations*", and paragraphs 7.12 to 7.14 make provision requiring "*internal approval to conduct operations under that authorisation in respect of equipment interference*".

iii) Paragraph 7.12 provides for internal approval of operations authorised under section 7 ISA by a "*designated senior official*".

Arrangements

24. Some limited parts of the internal 'arrangements' of GCHQ have been disclosed. In summary:

a) The "Compliance Guide – Authorisations" states: "*The ISA warrant and authorisations scheme is a mechanism for removing liability that would otherwise attach to interference with property such as computers, phones and routers. This interference would otherwise be a criminal offence under the Computer Misuse Act.*" In other words, the Respondents accept that in the absence of a valid authorisation, CNE violates domestic law [DD/1].

b) That Compliance Guide also states in relation to section 7 ISA: "*An ISA s.7 authorisation may be specific to a particular operation or target, or may relate to a broad class of operations. Wherever possible, GCHQ seeks to rely on class authorisations, including a class authorisation which permits interference with computers and communication systems overseas and removes liability under the Computer Misuse Act 1990 for interference with target computers or related equipment overseas (for this sort of activity, it is the location of the target computer which is relevant.*"

c) In contrast, the section in relation to section 5 ISA makes no reference to the possibility of a warrant covering "*a broad class of operations*"; and,

d) An extract from the current Advanced Training for Active Operations states: "*CNE operations must be authorised under ISA s.5 or s.7, depending whether the target computer or network is located within or outside the British Islands.*" The Guidance also notes the 5-day grace period under section 7, if the target computer is brought into the British Islands.

Annex 2 – Submissions of the Law Society in *DRIPA* litigation

IN THE COURT OF APPEAL **APPEAL NO C1/2015/2613**
ON APPEAL FROM THE DIVISIONAL COURT
Bean LJ and Collins J

BETWEEN:

R (OAO (1) DAVID DAVIS MP, (2) TOM WATSON MP)

Claimants

-and-

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Defendant

SUBMISSIONS ON BEHALF OF
THE LAW SOCIETY OF ENGLAND AND WALES

---

1. One of the factors that led the Court of Justice of the European Union in *Digital Rights Ireland* (Case C-293/12) to hold that Directive 2006/24 was contrary to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("the Charter") was the absence of any exceptions in the Data Retention Directive for data relating to persons, *"whose communications are subject, according to rules of national law, to the obligation of professional secrecy."* (§58 emphasis supplied)

2. Likewise, neither the Data Retention and Investigatory Powers Act 2014 ("DRIPA") nor the Regulation of Investigatory Powers Act 2000, which governs access to communications data retained under DRIPA ("RIPA"), include any exemptions in respect of persons subject to professional obligations of secrecy.

3. In her Detailed Grounds for Contesting the Claim at §85, the Home Secretary makes three claims:

(1) First, that DRIPA, *"does not extend to the content of any communications and consequently do not involved any interference with obligations of professional secrecy or confidence…."*

(2) Second, that *"the ability to use any data that did interfere with those interests in subsequent legal proceedings would be limited…"*.

(3) Third, that the Government has amended the draft RIPA Acquisition and Disclosure Code of Practice 2007, *"to impose additional considerations as part of the process where it is known that communications data discloses contact between persons of certain professions and those they are advising".*

4. The Acquisition and Disclosure Code of Practice 2007 (revised) – which is not legally binding and does not have the force of statute – now provides in paragraphs 3.72 – 3.74 that, *"special consideration to necessity and proportionality"* must be given when seeking communications data relating to a person who is a member of a profession that handles privileged or otherwise confidential information. Furthermore, *"particular care"* must be taken by designated persons when considering such applications.

5. It is also said that it *"may be possible to infer"* an "issue of sensitivity" from the fact that a person has regular contact with a lawyer, journalist, doctor, minister of religion or Member of Parliament.

6. This guidance is prefaced with the statement that:

> "Communications data are not subject to any form of professional privilege – the fact that a communication took place does not disclose what was discussed, considered or advised."

7. Therefore not only are there no restrictions on the ability of persons to acquire communications data that is protected by professional confidence or legal professional privilege, but any person applying the revised Acquisition and Disclosure Code of Practice would conclude (1) that disclosure of communications data cannot infringe legal professional privilege; (2) that communications with lawyers have equivalent status in domestic law as communications with journalists, doctors, Ministers of religion (etc), and (3) that the sensitivity of communications with lawyers is a matter which merely requires particular care to be taken and *"special consideration"* (a vague notion) given to issues of necessity and proportionality.

8. The Law Society for England and Wales is concerned that these statements do not accurately reflect the obligations of professional secrecy recognised and upheld by the common law between a lawyer and their client.

9. Taking the Secretary of State's second point first, the fact that there are restrictions on the ability to use legally privileged material in legal proceedings fails to address the fact that legal professional privilege is a substantive right and not a mere rule of evidence. It provides an assurance of complete confidentiality in obtaining legal advice, and dealing with legal advisers in the context of litigation, and not merely an assurance that the communications will not be deployed in legal proceedings.

10. Thus:

(1) In *R v Derby Magistrates Court, Ex p. B* [1996] AC 487 at 507 Lord Taylor of Gosforth stated:

> "…a man must be able to consult his lawyer in confidence, since otherwise he might hold back half the truth. The

client must be sure that what he tells his lawyer in confidence will never be revealed without his consent. Legal professional privilege is thus much more than an ordinary rule of evidence, limited in its application to the facts of a particular case. It is a fundamental condition on which the administration of justice as a whole rests."

(2) In *R (Morgan Grenfell & CO Ltd) v Special Commr of Income Tax* [2002] UKHL 21, [2003] 1 AC 563, 606-607 §7 Lord Hoffmann stated:

> "LLP is a fundamental human right long established in the common law. It is a necessary corollary of the right of any person to obtain skilled advice about the law. Such advice cannot effectively be obtained unless the client is able to put all the facts before the adviser without fear that they may afterwards be disclosed and used to his prejudice."

11. As to the first and third points advanced by the Secretary of State, whilst it is generally the case that legal professional privilege attaches only to the content of communications and will not cover records of attendance or the identity of client[9] this is by no means always so. Legal professional privilege will apply to information that may identify a client or their location, or the timing and frequency of contact with the lawyer, where such information is confidential.

12. Thus, information such as the dates of letters between solicitors and their clients have been held to be privileged because of the risk that their contents may be inferred: *Gardner v Irvin* (1878) 4 Ex D 49 at 83 (Cotton LJ).:

> "I think that the plaintiffs are not entitled to have the dates of the letters and such other particulars of the

[9] *R v Manchester Crown Court ex p. Roberts* [1999] 1 WLR 832 at 839 C-F: "A record of appointment made does involve a communication between the client and the solicitors' office but is not in my judgment, without more, to be regarded as made in connection with legal advice." (Bingham CJ).

> correspondence as may enable them to discover indirectly the contents of the letters, and thus to cause the defendants to furnish evidence against themselves in this action." (approved *Derby v Weldon (No 7)* [1990] 1 WLR 1156)

13. This principle has been recognised as having wider application in several recent cases where the identity of a client and other information about them, such as their whereabouts or information which might indicate their movements, has been held to be protected by privilege. The underlying rationale is that if such information is not protected absolutely, some individuals would be deterred from contacting lawyers and obtaining legal assistance.

14. In *JSC BTA Bank v Solodchenko & Ors (No 3)* [2011] EWHC 2163, [2013] Ch 1 Mr Justice Henderson held that where a solicitor's client had provided his contact details under conditions of confidentiality, the justification for recognising legal professional privilege, namely, that a person should not be inhibited in seeking the aid of a lawyer, was just as squarely engaged as in relation to the advice itself. He said at §19:

> "I can think of few things more likely to inhibit the exercise by a client of his fundamental right to seek legal advice than an order requiring his solicitor to disclose to an adverse party contact details which were supplied to the solicitor in strict confidence and for the sole purpose of enabling the client to communicate with the solicitor. In my view any such order would tend to undermine the relationship of confidence which must subsist between solicitor and client if the client is to be able to unburden himself freely to the solicitor."

15. In *JSC Bank v Addleshaw Goddard LLP* [2012] EWHC 1252 (Comm) the Claimants sought details of a conference call facility and of a special email account maintained by a firm of solicitors in order to communicate securely with their client, who was evading justice. It was submitted that the lines of communication between the solicitors and their clients were not themselves privileged or confidential (§16). The Court accepted that *without more* records of

appointments and contact details do not attract legal professional privilege. But on the facts of that case it held:

> "The number and address have been provided by Addleshaw Goddard to the First Defendant in confidence. In my judgment the connections between the telephone number and the email address and the seeking and receiving of legal advice in the present case is clear and manifest." (§24)

16. Teare J held that despite the fact that the Defendant had gone into hiding in order to frustrate orders of the court, the right to have access to legal advice trumped this consideration. The Defendant was not an outlaw (§38).

17. Finally, in *SRJ Person(S) Unknown being the author and commentators of Internet Blogs, D & Co* [2014] EWHC 2293 (QB) Sir David Eady sitting as a High Court Judge dismissed an application for an order requiring solicitors to disclose the identity of their client. The information was sought by a company which had been the subject of leaks of confidential information on internet blogs by the anonymous employee, who was in breach of a court order. Sir David Eadie concluded:

> "the information as to the Defendant's identity was indeed the subject of legal professional privilege and thus protected … Even if it were not there are powerful reasons not to override the duty of confidence. It was not simply a piece of neutral background information, as would generally be the case with a client's name, since both he and his solicitor were well aware that the Claimant was keen to establish his identity …". (§27)

18. The ability to obtain communications data relating to or revealing the contact that a lawyer has had with his or her client squarely engages the authorities referred to above. Those authorities make clear that such information can be protected by legal professional privilege and revealing such information would in some cases represent a violation of the fundamental right of every person to obtain legal representation without fear or inhibition.

19. It is of great importance that individuals are able to speak to their legal advisers without fear that such communications will be obtainable and capable of being used against their interests. That would have a chilling effect on the obtaining of legal advice and assistance.

20. The right to confidentiality between lawyer and client is deeply ingrained in the common law and it is absolute. It is, *"the highest privilege recognised by the courts."* (C. Passmore 1-005, *Privilege* 3rd ed. 2013, p.5). It is more fundamental even than the right of journalists to protection of their sources or of a Member of Parliament to speak openly with a constituent.

Conclusion

21. In *Digital Rights Ireland*, the CJEU indicated that any compulsory data retention regime must be accompanied by adequate restrictions on access to information which is protected by professional confidence under national law.

22. The law of England and Wales recognises that communications data relating to dealings between lawyers and their clients will in many cases be subject to legal professional privilege and affords that right the highest status.

23. Despite this, there are no restrictions on access to such data under applicable legislation. The non-statutory guidance provided in the revised Acquisition and Disclosure Code of Practice wrongly asserts that legal professional privilege cannot apply to communications data, fails to make clear the particular status of legal professional privilege and sets out no clear or appreciable limits on access to such material. It clearly falls short of the requirements contemplated by the CJEU.

TOM HICKMAN
Blackstone Chambers

7 October 2015