IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

Claim No: CO/1052/2017

BETWEEN:

THE QUEEN
on the application of
LIBERTY

Claimant

- and -

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

Defendants

RE-RE-AMENDED STATEMENT OF FACTS AND GROUNDS FOR JUDICIAL REVIEW

References in this Re-Re-Amended Statement of Facts and Grounds for Judicial Review ("RRASFG") to the Permission Bundle take the form "CB/*x*/*y*/*z*", where "*x*" is the volume, "*y*" is the tab and "*z*" is the page number. As permission was granted in part on 14 July 2017, there has been a substantive hearing on that part of the claim, and there have been other relevant statutory developments, two additional volumes to those initially served (volumes 2B and 3) are included.

A SUMMARY OF CLAIM

1. The Claimant ("**Liberty**") seeks judicial review of certain provisions in the Investigatory Powers Act 2016 (the "**Act**") that provide for the interception of calls, emails and all other electronic communications, permit interference with electronic devices to obtain personal and other data, require third parties to retain data about communications (so that government can access it) or permit government to retain large sets of personal and other data. These provisions permit access to and retention of the content of communications, and other information about communications, on an unprecedented scale. They have

profound and far reaching human rights and privacy implications. They are incompatible with Articles 8, ~~and~~ 10 and 14 of the European Convention on Human Rights ("**ECHR**") and with EU law.

(1) Liberty

2. Liberty, formally the National Council for Civil Liberties, is a campaigning organisation that has long been concerned with privacy and surveillance issues. It has raised these concerns through lobbying, including in relation to the Act, and through past successful challenges in the European Court of Human Rights and the Court of Justice of the European Communities to United Kingdom interception and data retention provisions.

3. Liberty brought the successful challenge to a previous communications interception regime, s 3(2) of the Interception of Communications Act 1985, in *Liberty v United Kingdom*.[1] It is currently challenging a precursor provision to the bulk interception regime in the Act (s 8(4) of the Regulation of Investigatory Powers Act 2000 ("**RIPA**")) in *10 Human Rights Organisations v United Kingdom*[2] and was party to a challenge to these provisions before the Investigatory Powers Tribunal ("**IPT**").

4. Additionally, Liberty represent~~sed~~ Mr Tom Watson MP in his ~~ongoing~~ challenge to the compatibility with EU law of the Data Retention and Investigatory Powers Act 2014 ("**DRIPA**"). This challenge led to the decision of the Court of Justice ("**CJEU**") in the joined cases *Tele2 Sverige AB v Post- och telestyrelsen* (Case C-203/15) and *R (Watson) v Secretary of State for the Home Department* (Case C-698/15) ("***Watson***"),[3] which lays down mandatory requirements of EU law in relation to the retention of and government access to communications data.

5. Liberty relies on the witness statement of Silkie Carlo ("**Carlo 1**") **[CB/1/Tab 2]**, formerly a Policy Officer at Liberty specialising in technology and surveillance, as to Liberty's interest in this claim and for general background matters. She explains Liberty's particular involvement with the Act, which includes advocating for amendments, meeting with Ministers, the Opposition, other Members of Parliament and

---

1 App No 58243/00, 1 July 2008, Fourth Section.

2 App No 24960/15, pending.

3 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and R (Watson) v Secretary of State for the Home Department* ECLI:EU:C:2016:970.

Peers involved with the Act during its passage as well as the Terrorism Reviewer, giving written and oral evidence to the Joint Committee on the Investigatory Powers Bill (including oral evidence in in December 2015) and to the Public Bill Committee in March 2016, meeting with other civil society groups, and preparing briefings at each stage of the Act's passage through Parliament **('Carlo 1' [15]) [CB/1/2/pp.110-111]**.

5A. Liberty relies also upon the First and Second Witness Statements of Corey Lynn Stoughton dated 15 January 2018 ("**Stoughton 1**") and 8 February 2018 ("**Stoughton 2**") respectively, the First Witness Statement of Colin John Passmore dated 12 January 2018 ("**Passmore 1**"), and the First Witness Statement of George Danezis dated 29 June 2018 ("**Danezis 1**"). For the avoidance of any doubt, Liberty further relies on the other witness statements it has served to date in this claim, on the materials the Defendants have disclosed pursuant to their duty of candour, and on the skeleton arguments it has served to date.

(2) Basis of claim and relief sought

6. Liberty challenges:

(1) The "bulk" powers in Chapter 6 of the Act, namely, the power to issue bulk interception warrants in Chapter 6 Part 1, the power to issue bulk acquisition warrants in Chapter 6 Part 2, and the power to issue bulk equipment interference ("bulk hacking") warrants in Chapter 6 Part 3;

(2) The "thematic" equipment interference (hacking) power in Chapter 5 of the Act, insofar as it applies other than to a single person or premises;

(3) The power to issue retention notices to telecommunications operators requiring them to retain communications data under Part 4 of the Act (read with Part 3 and Part 6 Chapter 2);[4] and

(4) The power to retain "bulk personal datasets" under Part 7 of the Act.

[4] Part 3 provides directly for government access to such data. A bulk acquisition warrant under Part 6 Chapter 2 could be used by the government to obtain and retain data that a telecommunications operator is obliged to retain under a Part 4 retention notice.

7. The challenged provisions are incompatible with both Articles 8 and 10 (and in some cases Article 14) of the ECHR and EU law in summary because they:

(1) Permit the indiscriminate retention of data, including personal data, such as the content of electronic communications (eg calls and emails), information about electronic communications (eg call lists and web browsing history) and other related data;

(2) Each lack any requirement that an individual (or single set of premises) is identified as the subject of surveillance or interception and/or lack any requirement for reasonable suspicion in relation to the person about whom data is gathered (who need not be the subject of surveillance, as where surveillance of A gathers information about B's crime);

(3) Generally lack sufficient safeguards in relation to the obtaining of and access to the content of communications, other information obtained and data about communications (and in some cases discriminate unjustifiably between those of UK nationality, national origin and residency and others); and/or

(4) Lack sufficient safeguards specifically to protect journalistic sources and legally privileged material. For example:

(a) The bulk acquisition provisions (Part 6 Chapter 2) do not contain any express provisions on confidential journalistic sources or legally privileged material at all;[4a]

(b) None of the impugned provisions (or the codes of practice under them) require independent judicial determination of whether material is confidential journalistic material or a legally privileged communication prior to its being obtaining or used, nor do they make adequate provision in relation to subsequent use of such materials once obtained.

[4a] The relevant code of practice makes only general provision (referring to the possibility of "additional sensitivity") for legally privileged materials and makes limited and inadequate provision in relation to confidential journalistic sources, as explained below.

8. Liberty therefore seeks:

   (1) An order for the disapplication of the impugned provisions, on the basis that they are incompatible with EU law (and, to the extent necessary, on the basis of its right to an effective remedy under CFR Article 47); and/or

   (2) If and to the extent that the impugned provisions are not disapplied, a declaration under s 4 of the Human Rights Act 1998 that the impugned provisions are incompatible with Articles 8 and 10 of the ECHR.

9. Liberty anticipates that an order for disapplication of the impugned provisions due to incompatibility with EU law will be suspended to give the government an opportunity to comply with the Court's decision, as recently occurred in the successful challenge to DRIPA in *Watson*.[5] If and to the extent that the impugned provisions have had or will have any application (before an order for disapplication takes effect or otherwise), a declaration of incompatibility with Articles 8 and 10 should also be made.

B BACKGROUND AND PROCEDURAL HISTORY

(1) The practical effect of the provisions under challenge

10. Ms Carlo, Ms Stoughton and Mr Passmore sets out the relevant background to Liberty's concerns about the Act **[CB/1/2, CB/3/135-149, CB/3/127-134]**. In summary, Liberty is concerned that the impugned powers:

   (1) Allow the State unduly expansive secret electronic surveillance over those who are not suspected of any wrongdoing and whose information is not relevant to any wrongdoing;

   (2) Empower the State to gather and retain sensitive personal data in relation to each and every citizen in the UK concerning, amongst other things, health conditions, political opinions, personal relationships, people with whom they associate, sexuality, habits, daily routines and religious beliefs;

---

[5] *R (Davis & Watson) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) [122] (Bean LJ). The order made on 15 July 2015 was suspended until 31 March 2016.

(3) Empower the State to build a detailed picture of each citizen's personality, thoughts and activities;

(4) Fundamentally alter the relationship between citizens and the State, in particular in relation to electronic information — the default position will become that the State retains and can access all and any electronically stored or transmitted information;

(5) Deny citizens any privacy in relation to matters over which citizens ought to, and assume they will, have privacy;

(6) Result in a real and far-reaching impediment to the exercise of free speech rights to impart and receive information, including by encouraging self-censorship over the matters individuals communicate on and search for over the internet;

(7) Have a chilling effect on behaviour that is necessary for the proper functioning of civil society, including the ability to maintain privacy and to express views without government knowing of or having access to them.

11. The Act will have a significant impact upon Liberty itself. As Ms Carlo explains, the organisation's work includes (Carlo 1[9]) **[CB/1/2/p108]**:

(1) sensitive lobbying (including regular private meetings with parliamentarians and ministers);

(2) responding to government consultations and providing expert written and oral evidence to parliamentary committees on issues which have implications for human rights and civil liberties;

(3) involvement in private and public law litigation (both domestically and in the Court of Justice of the European Union/European Court of Human Rights) against state bodies such as police forces, the Security Service, the Secret Intelligence Service, GCHQ, Home Office, and Ministry of Defence;

(4) advising and acting for whistleblowers;

(5) undertaking investigative projects; and

(6) organising and facilitating public campaigns activism and public demonstrations.

12. Ms Carlo further explains that each of these activities is likely to be adversely affected or discouraged by the existence and exercise of the wide powers under the Act (Carlo 1 13–14]) **[CB/1/2/p110]**.

13. In addition, Liberty operates a public advice service that receives and responds to several thousand requests every year for legal and practical advice in relation to human rights and public law matters, which, by definition, usually involve the State and challenges to its actions (Carlo 1 [10, 33]) **[CB/1/2/p108 & p117]**.

14. For many if not all of the activities mentioned above, Liberty also provides and receives legal advice and communications and receives communications on other matters that are subject to legal privilege (Carlo 1 [33]) **[CB/1/2/p117]**.

15. More generally, Liberty employs staff who in the course of their work communicate by phone, both mobile and fixed line, and e-mail (Carlo 1[66]) **[CB/1/2/p131]**. Staff use platforms such as Skype to communicate with others, including individuals at risk of persecution, both in the United Kingdom and abroad. Liberty's staff work on computers that are connected to the internet and access the internet in the course of employment related research. Some members of Liberty's staff regularly travel overseas and work from there, including making calls (via telephone and online media such as Skype). As a result of their employment, staff members may have their data recorded in datasets that may be acquired and/or retained by one of the intelligence services under Part 7 of the Act.

16. Ms Carlo anticipates that all of these matters will be harder to carry out, less effective or will (need to be) done in ways that do not involve or minimise electronic communications and the use of electronic devices altogether in light of the Act (see, eg, Carlo 1 [62–63]) **[CB/1/2/p130]**.

17. In the circumstances, Liberty, Liberty's staff, members and its contacts are directly affected by the impugned provisions. To achieve its objects in light of the Act, Liberty has already begun to and will have to adapt further its behaviour and communications practices.

(2) The provisions under challenge

18. Liberty challenges the provisions of the Act summarised below:

(1) Part 6 Chapter 1, which permits the Secretary of State to issue "**bulk interception warrants**". These warrants permit or require the interception of (access to) the content of communications during their transmission or while stored so long as the "*main purpose*" of the warrant is to intercept "*overseas-related communications*" (broadly, those sent from or to individuals outside the British Islands) and the warrant is considered necessary and proportionate in the interests of national security (or in the interests of national security and for the purpose of preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security).[6] They also permit the disclosure and retention of that content, its "*selection for examination*" and its examination. Public disclosure of the existence of these warrants, steps taken to implement them or material obtained under them is an offence.

(2) Part 6 Chapter 2, which permits the Secretary of State to issue "**bulk acquisition warrants**". These warrants permit or require their addressee — a "*telecommunications operator*" (ranging from a public company such as British Telecom to a café offering customers access to wi-fi)[7] — to disclose or obtain and disclose "*communications data*" (broadly, data about a communication other than its "*content*", such as the time, duration and medium of the communication or an internet connection record)[8] where it is considered necessary and proportionate in

---

6 A warrant may be considered necessary on the ground of "economic well-being" only where it is necessary for obtaining information relating to the acts or intentions of persons outside the British Islands: s 138(3).

7 See the very broad definition of "*telecommunications operator*" and "*telecommunications service*" in s 261(10)–(11).

8 A technical and complicated definition of "*communications data*" is set out in s 261(5), by reference to other concepts defined in that provision and elsewhere. Broadly, "communications data" is data about persons or things (entities) or entities engaging in a specific activity at a specific time (events) which: (1) is (capable of being) held or obtained by (or on behalf of) a telecommunications operator and (a) relates to use of a telecommunications service or telecommunications system or (b) is about an entity to which a telecommunications service is provided and relates to that service or (c) is somehow attached to or logically associated with a communication for the purposes of a telecommunications system by which it is transmitted; or (2) is available directly from a telecommunications system and is somehow attached to or logically associated with a communication for the purposes of a telecommunications system by which it is transmitted; or (3) is (capable of being) held or obtained by (or on behalf of) a telecommunications operator, is about the

the interests of national security (or in the interests of national security and for the purpose of preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security).[9] They also permit the disclosure and retention of the communications data, its "*selection for examination*" and its examination. Public disclosure of the existence or contents of these warrants by a telecommunications operator is an offence.

(3) Part 6 Chapter 3, which permits the Secretary of State to issue "**bulk equipment interference warrants**" (commonly known as "bulk hacking warrants"). These warrants permit or require the interference with any equipment for the purpose of obtaining any information (including the content of communications) so long as the "*main purpose*" of the warrant is to obtain "*overseas related communications*", "*overseas-related information*", or "*overseas-related equipment data*". The warrant must be considered necessary and proportionate in the interests of national security (or national security and for the purpose of preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security).[10] A bulk equipment interference warrant does not permit interception of communications during their transmission, for which a Part 6 Chapter 1 warrant is necessary.[11] Bulk equipment interference warrants also permit the disclosure and retention of that content, its "*selection for examination*" and its examination. Public disclosure of the existence of these warrants, steps taken to implement them or material obtained under them is an offence.

---

architecture of a telecommunications system and is not about a specific person. However, "*communications data*" does not include the "*content*" of a communication (or "*systems data*" that would be "*content*" if it were not excluded from the definition of content). "*Content*" is defined in s 261(6) as any element of a communication (or attached/associated data) that "*reveals anything of what might reasonably be considered to be the meaning (if any) of that communication*", but excluding anything that is "*systems data*" (relevantly, data that enables or facilitates the functioning of a telecommunications system: s 263(4)) or "*any meaning arising from the fact of the communication or from any data relating to the transmission of the communication*".

9 A warrant may be considered necessary on the ground of "economic well-being" only where it is necessary for obtaining information relating to the acts or intentions of persons outside the British Islands: s 158(3).

10 A warrant may be considered necessary on the ground of "economic well-being" only where it is necessary for obtaining information relating to the acts or intentions of persons outside the British Islands: s 178(3).

11 However, warrants can be combined: see s 248 and Schedule 8.

(4) Part 5, which permits the Secretary of State to issue "**targeted equipment interference warrants**" (commonly known as "targeted hacking warrants"). These warrants permit or require the interference with any equipment for the purpose of obtaining any information (including the content of communications). In addition, they must be considered necessary and proportionate: in the interests of national security; for the purpose of preventing or detecting serious crime; in the economic interests of the United Kingdom insofar as these are also relevant to the interests of national security; or preventing death or preventing or mitigating any injury or damage to a person's physical or mental health (ss 102, 106). Under s 101, they must relate to equipment which is specified by reference to its connection with certain persons, groups or locations. Liberty challenges Part 5 only insofar as it permits warrants under s 101(1)(b)–(h), that is, the power under Part 5 to issue warrants to interfere with equipment in very broadly defined categories, and that under s 101(1)(a) insofar as it does not require reasonable suspicion.[12] Again, public disclosure of the existence of these warrants, steps taken to implement them or material obtained under them is an offence.

(5) Part 4 (read with Part 3 and Part 6 Chapter 2), which permits the Secretary of State to issue a "**retention notice**". A retention notice requires (one or many) telecommunications operators to retain (potentially all) "*relevant communications data*" of any description.[13] It must be considered necessary and proportionate for any of a wide range of purposes or interests: the interests of national security; the

---

12 ~~Accordingly,~~ Liberty makes this more limited ~~does not at present~~ challenge to the power in Part 5 to issue warrants under s 101(1)(a) to interfere with equipment that belongs to, is used by or is in the possession of a particular person or organisation.

13 By s 87(11), "*relevant communications data*" is communications data that may be used to identify or assist in identifying any of the sender/recipient of a communication (whether or not a person), the time or duration of a communication, the type/method/pattern, or fact, of a communication, (part of) the telecommunications system through or by which a communication is/may be transmitted or the location of any such system. It expressly includes "*internet connection records*", which appear to include at the very least records of websites visited and, in Liberty's view, extend also to individual pages viewed. Section 62(7) defines "*internet connection records*" as communications data which (a) may be used to identify or assist in identifying a telecommunications service (such as a website) to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to or running a computer file or program (for example, entering a web address into a browser on a computer connected to the internet) and (b) comprises data generated or processed by a telecommunications operator (such as the web address entered or packets of information sent) in the process of supplying the telecommunications service to the sender of the communication (such as providing access to the website entered or, more precisely, sending the content of that website to the individual browsing).

purpose of preventing or detecting (any) crime or preventing disorder; the interests of the economic well-being of the United Kingdom insofar as those interests are relevant to the interests of national security; the interests of public safety; the purpose of protecting public health; the purpose of assessing or collecting any tax, duty levy or any other payment to a government department; the purpose of preventing death or preventing or mitigating injury or any damage to a person's physical or mental health; to assist investigations into alleged miscarriages of justice; to assist in identifying persons or obtain information about their next of kin where they have died or are unable to identify themselves; or the purpose of exercising functions relating to the regulation of financial services and markets or financial stability (ss 61(7) and 87(1)(a)). (In consequence of Liberty's EU law challenge, amendments to Parts 3 and 4 to remove some of these purposes and to require independent authorisation of access to and use of communications data (in most cases) have been ~~laid before Parliament but not yet~~ made. Liberty addresses the ~~proposed~~ amendments below.) Part 3 is important context for Part 4, as it provides one means by which the data retained under Part 4 may be accessed. It appears that communications data retained under Part 4 might also be retained and accessed under a warrant under Part 6 Chapter 2.[14]

(6) Part 7, which permits the Secretary of State to issue a warrant permitting an intelligence service to retain a "**bulk personal dataset**", that is, a dataset that includes personal data, is of a nature such that the majority of individuals whose data is held are not and are unlikely to become of interest to the intelligence service, and is retained electronically for analysis in the exercise of the intelligence service's functions.[15] A warrant must be considered necessary and proportionate in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom

[14] There is no reason in principle why data retained under Part 4 could not be obtained under a warrant under Part 6 Chapter 1 (or, for that matter, Part 6 Chapter 3): insofar as Part 6 Chapter 1 permits a warrant for the main purpose of obtaining "*secondary data*" from overseas communications (ss 136(2)(b), 137) it could be intercepted when transmitted, and when stored it could be obtained under an equipment interference warrant under Part 6 Chapter 3.

[15] Warrants under Part 7 are either "*class BPD warrants*", which permit retention and examination of several bulk personal datasets of a certain description, or "*specific BPD warrants*", which permit retention and examination of one bulk personal dataset.

so far as those interests are also relevant to the interests of national security. Liberty challenges Part 7:

(a) in its application to datasets collected under the Act (under each of the powers mentioned above). This is because Part 7 enables any safeguards that would otherwise exist under Part 6 (save for under Part 6 Chapter 2),[16] Part 5 or Part 4 in relation to the retention and use of data to be disapplied and is therefore relevant to the assessment of their compatibility with ECHR Articles 8 and 10 and with EU law; and

(b) in addition, in and of itself, because it confers a power to retain personal data for vague and ill-defined purposes and otherwise lacks adequate safeguards.

19. Each of the impugned Parts or Chapters of the Act (save for Part 7) permits indiscriminate obtaining and retention of the content of communications, any kind of information, and/or detailed information about communications, for broad and/or wide-ranging purposes. Part 7 permits their continued retention for equally broad purposes.

20. The impugned provisions mentioned above each contain various safeguards. However, those safeguards are insufficient to make the impugned provisions compatible with Articles 8 and 10 ECHR and EU law. Certain of the safeguards also discriminate on the basis of nationality and/or national origin and/or residence without justification. The safeguards include:

(1) approval of the decision to issue a warrant or notice by a "*Judicial Commissioner*", but applying a judicial review standard, in circumstances where there is no requirement for the Secretary of State to give reasons for the decision, and without any opposition being presented to the decision;

(2) in some cases, requirements that "*arrangements*" exist in relation to the use, storage and destruction of communications, information and other data obtained. However,

[16] Section 225(2) prevents the application of Part 7 to a bulk personal dataset collected under a bulk acquisition warrant under Chapter 6 Part 2.

these are not set down in the Act ~~(and have not, so far as Liberty is aware, yet been created, whether as codes of practice under Schedule 7 to the Act or otherwise)~~;[17]

(3) general oversight of the exercise of functions under the Act under Part 8 by the Investigatory Powers Commissioner ("**IPCr**"); and

(4) a person's ability to apply to the Investigatory Powers Tribunal under RIPA s 65 and s 243 of the Act for investigation of the exercise of powers under the Act in relation to them, but only where a person has an evidential basis that supports something more than an "*asserted general belief*" or a "*potential risk*" that their communications have been monitored (that is, where they are aware of secret surveillance of their communications).[18]

21. As explained below in more detail, these safeguards, to the extent to which they apply to any of the impugned provisions, do not cure their inconsistency with Articles 8 and 10 ECHR and EU law. Further, some safeguards discriminate unjustifiably on the basis of nationality and/or national origin and/or residence, inconsistently with Article 14 ECHR ~~and EU law~~.

(3) Assent to the Act and commencement of the impugned provisions

22. The Act received Royal Assent on 29 November 2016. It is now, for the most part, in force.

23. ~~Save for Part 3 4, Part 6 Chapter 2 and Part 7, many Mostm~~ Most of its relevant provisions have now~~not yet~~ commenced (in particular ~~Part 5 is~~Part 6 Chapter 2 and Part 7 are ~~in large part~~ in force and Part 5, Part 6 Chapter 1 and Part 6 Chapter 3 have commenced in

---

17 Liberty understands that, on 23 February 2017, the government published draft codes of practice in relation to powers under the Act, including the impugned provisions (except for Part 4), for consultation. Final codes of practice for all impugned provisions ~~except Part 4~~ have been published as set out below in paragraph 31A(1). It remains unclear whether, but appears not to be the case that, these are intended to be ~~the only~~ "*arrangements*" to which the Act refers. As Liberty submits below, to the extent that any arrangements are not publicly accessible, they (their existence and their content) may not be relied upon, in relation to the ECHR or EU law, as part of the justification for the impugned provisions.

18 *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15-165-CH [45]–[47]; see also [12]. The ECtHR therefore proceeded on what can now be seen to be an incorrect basis when, in *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [190], it relied on "*the absence of any evidential burden to overcome in order to lodge an application with the IPT*".

their entirety).[19] The Defendants didhave not suggested in pre-action (or other) correspondence that, in consequence, grounds for review hadhave not yet arisen.[19a] The Defendants' previous pleadings in this claim had suggested that the remaining provisions would commence soon, in the months following December 2017 (see paragraph 29G(1) below). Codes of practice were made in relation to all of the impugned provisions (except for Part 4) on 8 March 2018 by the Investigatory Powers (Codes of Practice) Regulations 2018 (SI 2018/355) (see paragraph 31A(2) below). The Defendants have said in correspondence that a draft code of practice for Parts 3 and 4 was laid before Parliament on 28 June 2018, and such a Code of Practice was made on 31 October 2018: see paragraph 31A(3) below.

(4) Pre-action correspondence

24. On 20 December 2016, Liberty sent a letter to the First and Second Defendants under the Pre-Action Protocol for Judicial Review ("**Pre-Action Letter**") **[CB/1/3/pp141-180]**.

---

[19] Limited provisions have been brought into force. Part 4 has been brought into force as from 30 December 2016, albeit at that stage partially and, importantly, without the requirement for approval of retention notices by a Judicial Commissioner (but now in full): see as to the previous position Investigatory Powers Act 2016 (Commencement No 1 and Transitional Provisions) Regulations 2016 (SI 2016/1233) reg 2(c), which brought brings s 87(1)(a) but not s 87(1)(b) into force. Sections 227 and 228 (which provide for the appointment of the IPCr and Judicial Commissioners) commenced on 29 January 2017: s 272(3). OtherThe provisions that relate to Judicial Commissioners and codes of practice (amongst others) have since as from 13 February 2017 been brought into force by the Investigatory Powers Act 2016 (Commencement No 2 and Transitory Provision) Regulations 2017 (SI 2017/137). (A technical mistake in these regulations was corrected in the Investigatory Powers Act 2016 (Commencement No 2 and Transitory Provision) (Amendment) Regulations 2017 (SI 2017/143).) Further provisions again that relate to Judicial Commissioners and codes of practice (amongst others) have beenwere brought into force (in some cases for limited purposes) from 1 September 2017: Investigatory Powers Act 2016 (Commencement No 3 and Transitory, Transitional and Saving Provisions) Regulations 2017 (SI 2017/859) reg 2. On 12 March 2018, provisions were commenced that (amongst other things): permit the issue of technical capability notices by the Secretary of State (ss 253–258) and review of these by Judicial Commissioners (s 229); and confer jurisdiction on the IPT over retention notices under Part 4 (s 243(1)(c), inserting s 65(5)(czb), (czc) and (czl)–(czm) into RIPA) and technical capability notices (s 243(1)(c), inserting s 65(5)(czi), (czj) and (czl)–(czm) into RIPA): Investigatory Powers Act 2016 (Commencement No 4 and Transitional and Saving Provisions) Regulations 2018 (SI 2018/341) reg 2. Most recently, Part 5 (in large part), Chapter 6 Part 1 and Chapter 6 Part 3 were brought into force, in part from 31 May 2018 and fully (or in the case of Part 5 more fully) from 27 June 2018: Investigatory Powers Act 2016 (Commencement No 5 and Transitional and Saving Provisions) Regulations 2018 (SI 2018/652) regs 4–5, 9–10. Part 2 (amongst other provisions) has also commenced in part: reg 8. Part 6 Chapter 2 and Part 7 were brought into force in part from 25 July 2018 and will commenced in full from 22 August 2018: Investigatory Powers Act 2016 (Commencement No 7 and Transitional Saving Provisions) Regulations 2018 (SI 2018/873) regs 2–3. However, s 87(1)(b), which provides for review by Judicial Commissioners of retention notices under Part 4, remains not yet in force. A list of the commencement status of the provisions of the Act as at 3 August 201829 June 201827 February 2017 is at **[CB/2B/1/311]**.

[19a] On the position the Defendants took in their Summary Grounds of Resistance, see paragraph 29E below.

The letter set out the legal flaws in the impugned provisions of the IPA in relation to bulk interception (Part 6 Chapter 1), bulk and thematic hacking (Part 6 Chapter 3 and Part 5 respectively), bulk acquisition (Part 6 Chapter 2), and bulk personal datasets (Part 7). Liberty indicated that it considered it was entitled to an order for disapplication of the impugned provisions in EU law and/or a declaration of incompatibility with human rights under Article 8 of the ECHR. The letter indicated that it is in the public interest for a challenge to the impugned provisions to be brought promptly and that Liberty was, from its experience and interest, well-placed to bring such a challenge. Liberty requested a response by 6 January 2017.

25. The Defendants ~~have~~ failed to respond to the substance of that letter, by 6 January 2017 or at any time before Liberty commenced this claim~~and thereafter~~. Instead:

(1) On 23 December 2016, the Defendants, via the Government Legal Department ("**GLD**"), stated that they would revert by 6 January 2017 with a timetable for their response and indicated that, in light of the *Watson* judgment (which had come down that day), Liberty might wish to amend the Pre-Action Letter **[CB/1/3/p181]**;

(2) Liberty on 5 January 2016 suggested that the Defendants should have until 13 January 2017 to respond and that it would update the Pre-Action Letter in light of *Watson* **[CB/1/3/p182]**;

(3) Liberty on 9 January 2017 sent a revised version of the Pre-Action Letter, showing changes that had been made in light of *Watson* (the "***Watson* Update Letter**") **[CB/1/3/pp183-206]**;

(4) On 13 January 2017, the Defendants stated that the Government was giving "*urgent consideration to what action is required*" in light of *Watson* and stated that they were unable to say when they would provide a substantive response to the claim, save to say it would be as soon as possible **[CB/1/3/p207]**;

(5) On 16 January 2017, Liberty wrote to the Defendants inviting them to propose a reasonable extension for their reply in accordance with the Pre-Action Protocol and pointing out that Liberty's claim relied on the ECHR so, to that extent, was not directly affected by *Watson* **[CB/1/3/p208]**;

(6) On 27 January 2017, the Defendants responded by noting Liberty's position and stating: "*Our position on the timing of a substantive response to your letter before claim remains as previously set out.*" **[CB/1/3/p209]**

26. On 21 February 2017, Liberty sent a further letter to the Defendants (the "**Part 4 Update Letter**"), indicating its intention to challenge the provisions of Pt 4 of the Act (read with the Pt 3 and Pt 6 access regime) and seeking a response on procedural matters it had raised in the Pre-Action Letter on 23 December 2016 **[CB/1/3/pp210-223]**. Liberty understood by this point that, although the claimants in *Watson* would seek to have the Court of Appeal deal with their existing challenge to DRIPA and the provisions in the IPA (Pts 3 and 4) that have replaced (but substantively re-enact) them, they would not be challenging the general and indiscriminate retention of data for which Part 4 provides.

27. The Defendants responded on 23 February 2017 to say they would be unable to provide a reply to the Part 4 Update Letter on that day and that they were not in a position to agree that Liberty should receive permission **[CB/1/3/p224]**. The Defendants agreed that Liberty should submit its application for a costs-capping order after any decision to grant permission.

28. The Defendants ~~have~~ failed, at any point prior to the commencement of this claim, to respond to the substance of the Pre-Action Letter, the *Watson* Update Letter or the Part 4 Update Letter.

29. The Defendants ~~have~~ also failed to confirm that they are the appropriate Defendants, to respond to Liberty's requests to agree the permission and costs for a permission hearing, or to indicate when they might be in a position to respond substantively.

(5) The claim, the Defendants' Summary Grounds of Resistance and the Defendants' statements to Mr Watson

29A. Liberty brought this claim on 28 February 2017.

29B. The Defendants failed to file an Acknowledgement of Service ("**AoS**") not more than 21 days after service of the Claim Form, as required by CPR 54.8(2)(a). On 24 March 2017, the due date, the Defendants wrote to the Court seeking an extension of time. The Court

stated in response on 29 March 2017 that a formal application would be required for the Defendants to serve their AoS out of time.

29C. On 6 April 2017, the First Defendant, in a letter to Tom Watson MP, said that DRIPA was "*inconsistent with EU law because it did not contain prior judicial approval or independent administrative authorisation of applications for retained communications data, and the crime purpose for which data could be retained or acquired was not restricted to serious crime*" and that "*the Government will be bringing forward legislative changes to the Investigatory Powers Act in the light of the European Court of Justice's judgment* [in *Watson*]".

29D. The Defendants on 7 April 2017 filed an AoS **[CB/3/8-11]** Summary Grounds of Resistance ("**SGR**") **[CB/3/12-25]** and an application to extend the time in which their AoS and SGR could be filed. Liberty consented to that application. Mostyn J granted that application on 15 May 2017 **[CB/3/28]**.

29E. The SGR argued in summary that this claim was premature and permission should be refused because (SGR ¶¶2, 4, 41, 43):

(1) For those impugned provisions that were not then in force,[19b] relevant legal frameworks, in particular statutory codes of practice under Schedule 7 of the Act, had not yet been made; and

(2) In the case of Part 4, which was in force (and for which no statutory code of practice had been or since has been made), proposed legislative amendments to Part 4 were to be brought forward.

29F. SGR ¶5 stated that the Defendants did not accept that any part of the claim was arguable. However, the SGR did not respond to the substance of Liberty's Statement of Facts and Grounds (save for assertions to the contrary of some legal points or references to decisions of the IPT that the Defendants appeared to suggest to be relevant, as set out below).

29G. In relation to the commencement of the impugned provisions, the SGR stated that:

[19b] All but Part 4, that is, the provisions on bulk interception (Part 6 Chapter 1), bulk and "thematic" equipment interference (Part 6 Chapter 3 and Part 5), bulk acquisition of communications data (Part 6 Chapter 2) and bulk personal datasets (Part 7).

(1) The impugned provisions that were not then in force were expected to commence as follows:

Provision	**Timing**	**Reference**
Chapter 6 Part 1 (bulk interception)	"*not … before early 2018 (at the soonest)*"	SGR ¶11
Chapter 6 Part 2 (bulk acquisition of communications data)	"*not … before early 2018 (at the soonest)*"	SGR ¶17
Chapter 6 Part 3 (bulk hacking)	"*not … before early 2018 (at the soonest)*"	SGR ¶21
Chapter 5 (thematic hacking)	"*not … before early 2018 in relation to the security and intelligence agencies and the Ministry of Defence, and before April 2018 in relation to law enforcement agencies (at the soonest)*"	SGR ¶25
Chapter 7 (bulk personal datasets)	"*not … before March 2018 (at the earliest)*"	SGR ¶35
Part 3 (acquisition of retained communications data)	"*deferred until any necessary amendments are made*"	SGR ¶33

~~(The Defendants have not since indicated to the Court or to Liberty that any of these anticipated timings have changed and, as set out above, Part 5, Part 6 Chapter 1 and Part 6 Chapter 3 are now in force)~~;

(2) The Defendants intended that the impugned provisions that were not in force "*should come into force concurrently with, or after, the promulgation of statutory Codes of Practice governing the exercise of those powers*" (SGR ¶9);[19c]

(3) Internal guidelines in relation to bulk interception, bulk communications data retention, bulk equipment interference, "thematic" equipment interference and bulk personal datasets would be made after the codes of practice were made: SGR ¶¶11,

[19c] The Defendants indicated on 23 April 2018 that they intend that amendments will be made to Part 4 and brought into force by 1 November 2018, and that a code of practice for Part 4 will be made shortly before the amendments are made.

17, 21, 25, 35. (The Defendants contended that unpublished internal guidance is relevant to Liberty's challenge on ECHR grounds: SGR ¶41(3). This is wrong for the reasons in paragraphs 45–46B below.)

29H. On 2 May 2017, Liberty filed a Response to the SGR ("**Response**") **[CB/3/25(a)-25(l)]**. The Response explained in summary (Response ¶5) that:

(1) As Part 4 was in force, the challenge to Part 4 was not on any view premature;

(2) Codes of practice for the other impugned provisions were expected to be made within the coming months, so the rest of the claim should not be dismissed but should instead stayed until codes of practice were made; and

(3) The existence of other claims in the IPT or ECtHR that may, when decided, be relevant to the issues in this claim was no basis for refusing permission, all the more so where the Defendants' own argument was that the impugned provisions must be considered individually on their terms (Response ¶21(2)).

29I. Liberty proposed orders that would require the Defendants to state whether they conceded the claim in relation to Part 4 or any part of it and that would stay the remainder of the claim until the sooner of 1 February 2018 or approval by Parliament of any code of practice under Schedule 7 paragraph 4(4) of the IPA that relates to any of the impugned provisions (other than Part 4).

(6) The grant of permission

29J. On 14 July 2017, Jeremy Baker J (amongst other things) **[CB/3/86-88]**:

(1) Granted permission to Liberty with respect to the claim in relation to Part 4 of the Act (the "**Part 4 Claim**");

(2) Required the Defendants to set out in writing whether they intended to concede or resist the Part 4 Claim by 5 July 2017;

(3) Made directions for the hearing of the Part 4 Claim, in the event that it was contested, including for Liberty to file its application for a costs-capping order ("**CCO**");[19d]

(4) Stayed all other claims until the sooner of 28 February 2017 or approval by Parliament of a Code of Practice under Schedule 7 paragraph 4(4) of the Act that relates to the impugned provisions (other than Part 4);

(5) Required Liberty to notify the Defendants and Court in writing by 28 March 2018 whether the other claims are pursued and, if so, set out its further Grounds for Judicial Review.

(7) The Defendants' concessions that Part 4 is incompatible with EU law and their consequences

29K. On 7 July 2017, the Defendants stated in a letter to the Court **[CB/3/88(a)-(d)]**:

> "the Defendants do not contest the claim that Part 4 of the IPA is, in its current form, inconsistent with the requirements of EU law insofar as: (1) it does not ensure that, in the area of criminal investigations, access to and use of retained communications data is restricted to the objective of fighting serious crime; and (2) access to retained data is not subject to prior review by a court or an independent administrative body."

The Defendants stated that this was "*without prejudice to the question of the application of EU law in a national security context*".

29L. The Defendants stated that they would not contest the making of a declaration that Part 4 is inconsistent with EU law on these grounds, but denied that Liberty was entitled to any further order.

29M. On 13 July 2017, Liberty by letter requested from the Defendants further clarification of their position and responded to certain points **[CB/3/88(e)-(r)]**. Liberty noted in paragraph 2(2) that, by continuing to operate Part 4 having conceded it was incompatible with EU law, the Defendants' stance was "*contrary to law and show*[ed] *a disregard for the rights to privacy of citizens.*"

[19d] The period for this was originally set as 7 days from the Defendants' response. The Court, upon Liberty's application with the Defendants' consent, extended the date to 4 August 2017.

29N. On 26 July 2017, the Defendants responded to Liberty's letter **[CB/3/88(s)-(x)]**. Amongst other things, they denied in paragraph 2(b) that the Defendants were acting contrary to law by continuing to operate arrangements under Part 4.

29O. Liberty's Submissions in Support of a Costs Capping Order of 7 August 2017 ¶9(1) fn 5 responded in turn to this point as follows:

> "The Defendants contend that continuing to operate Part 4 to collect communications data, despite their concessions that Part 4 is incompatible with EU law, is not unlawful, because the CJEU's judgment '*did not disapply domestic primary legislation*' … This confuses legality and remedy. The CJEU's judgment in Watson explained the mandatory and directly applicable requirements of EU law — the requirements of Articles 7 and 8 of the EU Charter of Fundamental Rights (which have the same status as the Treaties) in the context of communications data retention and access. Accordingly, as a matter of EU law, and therefore English law under s 2(1) of the European Communities Act 1972, directly applicable requirements with Treaty status have '*the effect, in accordance with the principle of the precedence of EU law, in their relationship with the domestic law of the Member States, of rendering automatically inapplicable, merely by their entering into force, any conflicting provision of national law*': Case C-105/14 *Taricco* ECLI:EU:C:2015:555 [52]. Whether or not a Court exercises its inherent discretion to suspend an order for disapplication, by operating Part 4 the Defendants are acting contrary to EU and English law, so unlawfully."

So far as Liberty is aware, the Defendants have not at any point presented any reasoned response to this argument.

29P. For the avoidance of any doubt, Liberty's case was and remains that:

(1) any purported application of Part 4 to authorise the retention of communications data in circumstances where Part 4 is incompatible with EU law is unlawful; and

(2) any incompatibility with EU law has the consequence that, as a matter of law, Part 4 does not provide lawful authority for the imposition of requirements on telecommunications operators to retain communications data.

The same is true for any other of the impugned provisions insofar as they are incompatible with EU law.

(8) The making of the costs capping order ("CCO")

29Q. On 4 August 2017, Liberty filed an application for a CCO pursuant to Criminal Justice and Courts Act 2015 ss 88–89.

29R. On 4 October 2017, Lang J made a CCO in respect of the Part 4 Claim, which provideds that:

(1) The liability of the Claimant to pay the costs of the Defendants is limited to a total sum of £60,000 including VAT; and

(2) The joint liability of the Defendants to pay the Claimant's costs is limited to a total sum of £100,000, including VAT.

(8A) The challenge to Part 4 based on EU law is upheld in part

29S. The Part 4 Claim was listed for hearing for 27–28 February 2018 by a Divisional Court.

29T. By letters of 7 July 2017 (page 2), 28 July 2017 (paragraph 21) and 29 August 2017 (in paragraph 10), the Defendants made clear that:

(1) They had not made any code of practice under Part 4 of the Act (but intended to do so);

(2) The Defendants were continuing to "*have regard to the previous retention code of practice and the draft code (which covers both retention and acquisition of communications data) published during the parliamentary process for the Investigatory Powers Bill*"; and

(3) This was a reference respectively to the publications: Home Office, *Retention of Communications Data — Code of Practice* (March 2015) and Home Office, *Communications Data — DRAFT Code of Practice* (Autumn 2016).

29U. Liberty proposed on 25 October 2017, and the Defendants agreed on 14 November 2017, that the Part 4 Claim insofar as it was based on the ECHR should be stayed until after the February 2018 hearing.

29V. On 27–28 February, Singh LJ and Holgate J sitting as a Divisional Court heard the Part 4 Claim insofar as it was based on EU law (the **"Part 4 EU Law Claim**"). The Court handed down a procedural and a substantive judgment on 27 April 2017, respectively [2018] EWHC 976 (Admin) and [2018] EWHC 975 (Admin). It made orders and a declaration upholding the Part 4 EU Law Claim in part, staying elements of it, and dismissing it in part **[CB/3/260-264]**. The Divisional Court:

(1) Made the following declaration, by which the claim was allowed in part:

"IT IS DECLARED THAT:

1. Part 4 of the Investigatory Powers Act 2016 is incompatible with EU law in that (without prejudice to the application of EU law in a national security context) in the area of criminal justice:

(1) access to and use of retained data is not limited to the purpose of preventing and detecting serious crime; and

(2) access to retained data is not subject to prior review by a court or an independent administrative body.

2. Part 4 of the Investigatory Powers Act 2016 must be amended so as to remedy these incompatibilities within a reasonable time, being no later than by 1 November 2018."

(2) Declined to refer any question to the CJEU;

(3) Stayed the Part 4 EU Law Claim until the handing down of the CJEU's judgment in the reference made by the Investigatory Powers Tribunal in Case No IPT/151/110/CH (the "**IPT's Reference**") insofar as it concerns:

(a) the application of EU law in a national security context;

(b) any requirement under EU law to retain data within the EU; and

(c) any requirement under EU law to notify persons after data relating to them has been accessed or used;

(4) Otherwise dismissed the Part 4 EU Law Claim. Liberty accepts that these matters have been decided against it by the Divisional Court and does not by these

RRASFG suggest otherwise. Liberty maintains its pleaded case as to those aspects of the Part 4 EU Law Claim for the purposes of any application for permission to appeal, any appeal, and any application to the ECtHR;

(5) Extended the time for applications for permission to appeal against the dismissal of the Part 4 EU Law Claim to 21 days after the stayed aspects of the Part 4 EU Law Claim are disposed of or determined; and

(6) Required Liberty to file and serve any further Grounds for Review for the Part 4 Claim insofar as it is based on the ECHR (the "**Part 4 ECHR Claim**") if so advised within 28 days after the date on which a draft code of practice in relation to Part 4 is laid before Parliament under Schedule 7 of the Act (and required the Defendants to file and serve any further Detailed Grounds of Resistance within a further 28 days).

29W. ~~So far as Liberty is aware, no~~A code of practice in relation to Part 4 was~~has yet been~~ laid before Parliament on 28 June 2018. ~~Liberty is therefore not yet required to file any further Grounds for Review for the Part 4 ECHR Claim, pursuant to the orders of the Divisional Court made on 27 April 2018.~~Accordingly, Liberty ~~now~~ file~~d~~s the~~is~~ Re-Amended Statement of Facts and Grounds (after an extension) on 3 August 2018.

~~(9) Liberty is not aware of the Defendants' substantive position on~~ Permission is given on Liberty's challenge other than to Part 4

30. ~~In light of the matters set out above~~Accordingly, ~~Liberty does not know the Defendants' general position or their responses (if any) to the specific submissions below~~ After the Defendants filed Summary Grounds of Resistance on 28 September 2018, and Liberty filed a Response dated 2 November 2018 (on which it continues to rely and which should be taken to be incorporated herein), the Divisional Court by Order dated 27 November 2018 granted permission on the rest of the ~~Parts of its~~ claim other than the Part 4 Claim (those other parts hereinafter together called the "**Bulk Powers Claim**").

31. ~~In those circumstances, Liberty sets out its submissions below but may need to supplement this Statement of Facts and Grounds and file further evidence, including before consideration of permission, in light of any substantive response that may now be forthcoming.~~

31A. ~~In particular, there appears not to be any basis upon which the Defendants could suggest that the Bulk Powers Claim is premature and/or futile (or should not now proceed in the normal manner) given~~It is the case that:

(1) Part 5, Part 6 Chapter 1, Part 6 Chapter 2, ~~and~~ Part 6 Chapter 3 and Part 7 are now fully in force ~~(in some cases in part but soon in full)~~, and Part 4 is also in force (save in minor respects) as amended~~as explained above~~;

(2) Codes of practice were laid before Parliament on 18 December 2017 and made for all impugned provisions (other than Part 4) on 8 March 2018 by the Investigatory Powers (Codes of Practice) Regulations 2018 (SI 2018/355), as follows:

Impugned provisions	**Code of practice**
Chapter 6 Part 1 (bulk interception)	Home Office, *INTERCEPTION OF COMMUNICATIONS — DRAFT Code of Practice* (December 2017) **[CB/2B/2/44-179]** (the "**Bulk Interception CoP**")
Chapter 6 Part 2 (bulk acquisition of communications data)	Home Office, *Bulk Acquisition of Communications Data — DRAFT Code of Practice* (December 2017) **[CB/2B/2/180-234]** (the "**Bulk CD CoP**")
Chapter 6 Part 3 (bulk hacking) Chapter 5 (thematic hacking)	Home Office, *EQUIPMENT INTERFERENCE — DRAFT Code of Practice* (December 2017) **[CB/2B/2/235-378]** (the "**Bulk EI CoP**")
Chapter 7 (bulk personal datasets)	Home Office, *Intelligence Services' Retention and Use of Bulk Personal Datasets — DRAFT Code of Practice* (December 2017) **[CB/2B/2/379-445]** (the "**BPD CoP**")

(3) ~~The Defendants have not suggested that their expectations as to time of commencement of the impugned provisions (other than Parts 3 and 4 and Part 5, Part 6 Chapter 1 or Part 6 Chapter 3) set out in paragraph 29G(1) above have changed.~~A code of practice for Parts 3 and 4 was laid before Parliament on 28 June 2018, being Home Office, *Communications Data — DRAFT Code of Practice* (June 2018) **[CB/2B/2(i)/445.066]** (the "**CD CoP**"). Draft regulations to bring it into force ~~have also been~~ were laid before Parliament: draft Data Retention and

Acquisition Regulations 2018 reg 2 **[CB/2B/2(g)/445.001]**. Those regulations were made on 31 October 2018 and commenced on 1 November 2018.

~~If such a suggestion is made, Liberty will seek permission to respond by further submissions, before consideration of permission.~~

(10) The judgment of the Divisional Court on the ECHR Claim and the staying of the EU law aspects of the Bulk Powers Claim

31B. The Divisional Court rejected Liberty's challenge to the IPA based on ECHR grounds as set out herein: [2019] EWHC 2057 (Admin) (the "**ECHR Judgment**"). The time for appeal on those issues was extended pending judgment of the Grand Chamber of the ECtHR in the *Big Brother Watch* case (Application No 58170/13). Liberty's EHCR challenge as pleaded in this RRASFG is to be read in light of the ECHR Judgment. Liberty accepts that these matters have been decided against it by the Divisional Court and does not by this RRASFG suggest otherwise. Liberty maintains its pleaded case on the ECHR for the purposes of applications for permission to appeal, any appeal, and any application to the ECtHR.

31C. By consent, the EU law aspects of the Bulk Powers Challenge were not decided in the ECHR Judgment and instead stayed pending the decision on the preliminary reference to the CJEU in Case C-623/17 *Privacy International* ("*PI*").

(11) The CJEU's judgment is given in Case C-623/17

31D. The CJEU gave judgment in the reference in *PI* on 6 October 2020. On the same day, the CJEU gave judgment in Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net* ("*La Quadrature*").

31E. The parties agreed, by a consent order signed on 30 November 2020, that Liberty should have permission to amend the Re-Amended Statement of Facts and Grounds in relation to the EU law aspects of the claim. Liberty does so by the RRASFG.

C LAW

32. Liberty sets out below, in outline, the relevant ECHR and EU law principles.

(1) Articles 8 and 10 ECHR and secret surveillance

33. It is well established that legislation that provides for the secret interception of communications, such as the impugned provisions in Parts 4, 5 and 6 of the Act, interferes with rights, and must be capable of justification, under Article 8 ECHR. It is also well established that the retention by the State of such information interferes with, and must be justified under, Article 8 ECHR. The same applies under Article 10 ECHR.

(a) Interference

34. ECtHR case-law emphasises that that the interception or monitoring of telephone communications (including calls and SMSs), of email and of use of internet services (such as browsing history) by the state is a significant inference[20] with Article 8 rights to private and family life (of individuals) and to respect for correspondence (for individuals and legal persons)[21] under Article 8(1). So too is the obtaining of data that reveals an individual's movements.[22]

35. The existence of secret surveillance legislation, including through its chilling effect, constitutes in addition a serious interference with the rights to freedom of expression under Article 10 ECHR.[23] In considering Article 11 of the EU Charter of Fundamental Rights ("**CFR**") — which corresponds to Article 10 ECHR — in *Watson*, the CJEU stated:[24]

---

20 *Klass v Germany* (App No 5029/71, 6 September 1978, Plenary Court) [41] (telephone conversations); *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [79] (telephone conversations); *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [57] (interception, storage and listening to communications); *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [118] (mail, telephone and email communications); *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [117], [173] (mobile telephone communications, including SMS); *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [52]–[53] (electronic communications and computer data transmissions); *Copland v United Kingdom* (App No 62617/0, 3 April 2007, Fourth Section) [41] (telephone call data, email communication data and internet browsing history).

21 *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App No 62540/00, 30 January 2008, Fifth Section) [60].

22 *Uzun v Germany* (App No 35623/05, 2 September 2010, Fifth Section) [50]–[52], [66].

23 *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [80], [84], [89].

24 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [101].

> "Even if such legislation does not permit retention of the content of a communication … the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter …"

36. The rights under Articles 8 and 10 are, in the present context, interlinked such that interference with one entails interference with the other. As a UN Special Rapporteur recently concluded: "*States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy.*"[25] Ms Carlo explains the particular chilling effect on expression that Liberty anticipates from the invasion of and threat to privacy that the impugned provisions create, in particular due to the impossibility of confidential electronic communications under the Act and effect this has, for example, on journalists with whom Liberty works as well as the potential public interest litigants whom it represents (Carlo 1 [48, 61]) **[CB/1/2/p124 & p129]**.

37. Each of: the initial obtaining and examination of communications information by the state;[26] retention of that data;[27] the transmission, copying, disclosure, or further use of that data (such as listening to a recording or reading a transcript);[28] destruction of the data obtained and the failure to notify those monitored (which conceals monitoring measures),[29] is, in and of itself, "*a further separate interference*"[30] with Article 8(1) — and Article 10(1) — rights.

38. The Fourth Chamber recently emphasised the intensity of the interference in *Szabó*:[31]

---

25 *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue*, UN Doc A/HRC/23/40 (17 April 2013) [79].

26 *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [79]; *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [57].

27 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [255]; *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [57].

28 *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [79]; *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [57].

29 *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [79].

30 *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [79].

31 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [53], [70].

"Given the technological advances since the *Klass and Others* case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely …

The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile … of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 [which quoted *Digital Rights Ireland*[32]] and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices."

39. The ECtHR has consistently held that "*the mere existence of the … legislation* [permitting secret surveillance] *amounts in itself to an interference with the exercise of … rights under Article 8*",[33] because the "*menace of surveillance … necessarily strikes at freedom of communication*".[34] As such, Article 8 imposes constraints directly upon, and enables a challenge directly to, the law permitting surveillance. So too does Article 10.[35] The SGR rightly do not dispute that the impugned provisions interfere with the rights protected by Articles 8 and 10. Nor (correctly) do they suggest that Liberty cannot invoke both Article 8 and Article 10.

(b) Justification — Framework

40. To justify interference with Article 8(1) and 10(1) rights under Article 8(2) and 10(2), the interference must: pursue one of the legitimate aims mentioned in Articles 8(2) and 10(2); be "*in accordance with the law*" or "*prescribed by law*", that is, satisfy quality of

---

32 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* ECLI:EU:C:2014:238 [26], [27], [52], [62] ("Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238").

33 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [179]; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App No 62540/00, 30 January 2008, Fifth Section) [69].

34 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [53]; *Klass v Germany* (App No 5029/71, 6 September 1978, Plenary Court) [41].

35 *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [89].

law requirements; and be "*necessary in a democratic society*" (often referred to as "necessary and proportionate").

41. For abstract challenges to secret surveillance legislation under Articles 8 and 10, the requirements that interference be "*in accordance with the law*" or "*prescribed by law*" and "*necessary in a democratic society*" are "*closely related*" and often considered together.[36]

(c) Legitimate aims

42. Article 8(2) constrains the legitimate aims that secret surveillance legislation may pursue. These are: "*the interests of national security, public safety or the economic wellbeing of the country, ... the prevention of disorder or crime, for the protection of health or morals, or ... the protection of the rights and freedoms of others.*" Article 10(2) contains a similar set of legitimate aims: "*national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary*".

43. If legislation does not pursue one of these aims, it is incapable of justification under Articles 8(2) and 10(2). Any interference with Article 8(1) and 10(1) rights will be incompatible with Article 8 or Article 10.

(d) "In accordance with the law" — Accessibility and foreseeability/necessity

44. The requirement that an interference with Article 8(1) and 10(1) rights be "*in accordance with the law*" or "*prescribed by law*" means that the legal basis for the interference must be (1) accessible and (2) sufficiently clear or foreseeable.

Accessibility

45. The requirement of "*accessibility*" is that the law be published so as to be available to individuals. While "law" may encompass guidance on the exercise of functions, it does

[36] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [236]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [58]; *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [155].

not extend to "*the existence of a practice*".[37] (As explained below, any such guidance will be relevant only if and to the extent it is an effective constraint on the exercise of discretion under surveillance legislation.)

46. Accordingly, the Defendants may not rely upon any documents that are not publicly accessible (or to the extent they are not publicly accessible), whether purportedly binding or otherwise, in seeking to demonstrate that the Act is compatible with Articles 8 or 10.[38] For example, in *Liberty v United Kingdom*, in holding s 3(2) of the Interception of Communications Act 1985 incompatible with Article 8, the ECtHR did not take into account the United Kingdom's description of internal safeguards affecting interception of communications, because these were not public.[39]

46A. The Defendants contend in SGR ¶41(3), in reliance upon two decisions of the IPT,[39a] that:

(1) non-public "*internal practices and procedures*" are relevant in assessing whether there are sufficient safeguards against abuse; and

(2) Non-public and secret procedures put in place by agencies are relevant "*provided that what is publicly disclosed sufficiently indicates the scope of the agencies' discretion and manner of its exercise*".

46B. The Defendants fail to address the arguments and authorities set out in paragraphs 45–46 above. In any case, both of the propositions that the Defendants advance are wrong:

---

37 *Huvig v France* (App No 11105-84, 24 April 1990, Chamber) [34]; see also *Valenzuela Contreras v Spain* (App No 58/1997/842/1048, 30 July 1998, Judgment) [60] (details of the surveillance regime must be "*set out in detail in domestic law so that it has a binding force which circumscribes the judge's discretion in the application of such measures*").

38 See especially *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [240], [242]; *Leander v Sweden* (App No 9248/81, 26 March 1987, Chamber) [54]. If and to the extent that *Liberty v GCHQ (No 1)* [2014] UKIPTrib 13_77-H, [2015] HRLR 2 [39]–[41], [133(ii)] (Burton J) and *Privacy International v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib 15_110-CH [62] (Burton J) holds otherwise, they are~~it is~~ incorrectly decided, inconsistent with ECtHR case-law and should not be followed.

39 (App No 58243/00, 1 July 2008, Fourth Section) [48]–[51]. The United Kingdom's summary of its internal safeguards is described at [50]; the Court did not take them into account in its analysis at [66].

39a *Liberty v GCHQ (No 1)* [2014] UKIPTrib 13_77-H, [2015] HRLR 2 [39]–[41] (Burton J); *Privacy International v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib 15_110-CH [62] (Burton J).

(1) As set out in paragraph 45 above, the bare existence of a practice does not constitute "law" for the purposes of assessing the sufficiency of the safeguards of a secret surveillance regime: *Huvig v France*[39b] and *Valenzuela Contreras v Spain*.[39c] In any case, a practice does not in and of itself constrain the exercise of discretion. Accordingly, its existence cannot alter the conclusion that would otherwise follow as to whether a regime is in accordance with the law.

(2) The suggestion that non-public documents (even if "signposted") are relevant is inconsistent with decisions of the ECtHR in the context of secret surveillance regimes. In *Liberty v United Kingdom* (as explained in paragraph 46 above) the ECtHR did not take into account internal UK guidance which the UK described but which was not published. In *Zakharov v Russia*,[39d] the Court doubted that part of a law (its addenda) was accessible where those annexes were not officially published, even though they were available in full via an official magazine and via a proprietary online database. Unpublished guidelines not available in full to the general public are not accessible and therefore not relevant to whether a secret surveillance law has sufficient safeguards, on the ECtHR's approach.

(3) IPT decision in *Liberty v GCHQ (No 1)* relies only upon *Leander v Sweden*[39e] to suggest that non-public documents are relevant if sufficiently signposted. The IPT decision in *Privacy International v Secretary of State for the Foreign and Commonwealth Office* merely refers back to *Liberty v GCHQ (No 1)*.[39f] *Leander* concerned whether the framework for carrying out "*secret controls of staff in sectors affecting national security*" was sufficiently accessible, rather than a generally applicable surveillance regime.[39g] In any case, the ECtHR held that:[39h]

> "where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, **the law itself**, as **opposed to the**

[39b] (App No 11105-84, 24 April 1990, Chamber) [34].

[39c] (App No 58/1997/842/1048, 30 July 1998, Judgment) [60].

[39d] (App No 47143/06, 4 December 2015, Grand Chamber) [240], [242].

[39e] (App No 9248/81, 26 March 1987, Chamber) [51].

[39f] *Privacy International v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib 15_110-CH [62(ii)] (Burton J), which merely asserts that signposting is sufficient. The IPT refers at [60]–[61] and later in [62] to its decision in *Liberty v GCHQ (No 1)*.

[39g] *Leander v Sweden* (App No 9248/81, 26 March 1987, Chamber) [47]–[48], [51].

[39h] *Leander v Sweden* (App No 9248/81, 26 March 1987, Chamber) [51].

> **accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity**, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see the above-mentioned Malone judgment, Series A no 82, pp 32-33, §68)".

Further, in applying these principles, the ECtHR held that it could consider both the legislative framework and "*instructions issued by the Government*" about what details were to be included in a secret register (which circumscribed the discretion of the executive), but concluded:[39i]

> "However, of these [instructions] only one is public and hence sufficiently accessible to be taken into account, namely the Instruction of 22 September 1972 (see paragraph 20 above)."

Leander therefore provides no support for the legal proposition reached by the IPT. The IPT cases on which the Defendants rely are wrongly decided on this point and should not be followed.

Foreseeability/necessity

47. In the "*special context of secret measures of surveillance*", the requirement of foreseeability is that there are:[40]

> "clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures …"

48. Further, as surveillance measures are not open to scrutiny, the law must not confer "*an unfettered power*" to authorise surveillance and must "*indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with*

[39i] *Leander v Sweden* (App No 9248/81, 26 March 1987, Chamber) [54]. See [20]–[22], where the public and secret instructions are respectively set out and mentioned.

[40] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [229] (citations omitted) (emphasis added).

sufficient clarity to give the individual adequate protection against arbitrary interference".[41]

49. These are "*stricter requirements*" of foreseeability than generally apply under Article 8[42] or Article 10, which ordinarily require only that a law be "*formulated with sufficient precision to enable the individual — if need be with appropriate advice — to regulate his conduct*".[43] It is well-established that the stricter requirements apply to legislation permitting the obtaining and retention of and access to communications data[44] as well as to that permitting the obtaining content of communications (the text of emails or SMSes) or other information (for example, un-transmitted pictures stored on a mobile phone). All are serious interferences with Article 8 and 10 ECHR rights.

50. These strict foreseeability requirements apply under Article 10 as they do under Article 8: the quality of law requirement in Article 10(2) is "*identical in meaning*" to that under Article 8(2).[45]

51. The ECtHR's case-law establishes two elements of foreseeability that a surveillance law must satisfy, namely:

    (1) mandatory requirements of (1) individual targeting of surveillance measures and, in addition, (2) reasonable suspicion of the person about whom information is sought; and

    (2) setting out, with sufficient clarity and certainty, particular aspects of the powers to conduct electronic surveillance.

<u>Foreseeability/necessity — Mandatory requirements of individual targeting and reasonable suspicion</u>

52. The ECtHR's decisions in *Zakharov* and *Szabó* establish that, to satisfy the criterion of foreseeability, a surveillance law must require two things:

---

41 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [230] (citations omitted).

42 *RE v United Kingdom* (App No 62498/11, 27 October 2015, Fourth Section) [128].

43 *S and Marper v United Kingdom* (Applications Nos 30562/04 and 30566/04, 4 December 2008, Grand Chamber) [95].

44 *Liberty v GCHQ (No 1)* [2014] UKIPTrib 13_77-H [114] (Burton J).

45 *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [89]–[90].

(1) **Individual targeting:** An order or other act permitting surveillance must be limited to an identified individual or set of premises ~~or, perhaps, a single operation or investigation~~ (that is, an individual or~~,~~ set of premises ~~or operation/investigation~~ must be identified as the interception subject); and

(2) **Reasonable suspicion on sufficient factual basis:** Surveillance must be permitted only if there is a reasonable suspicion, on a sufficient factual basis, that the person about whom information is sought (who is not necessarily the interception subject) is engaging in acts that justify the imposition of surveillance (that is, acts that are relevant to the purposes for which surveillance may be imposed). For example, where a surveillance regime permits surveillance for the purposes of fighting serious crime, the regime must require that a reasonable suspicion exists that A ~~is~~ has engaged or will engage in serious crime, to impose surveillance upon A (and A's associate B) for the purpose of obtaining information about A's criminal activities.

53. As to the first of these requirements, individual targeting:

(1) In *Zakharov*, the Grand Chamber stated that an interception authorisation:[46]

> "must clearly define a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information …"

(2) Similarly, the Fourth Chamber in *Szabó* stated that secret surveillance must be "*strictly necessary*",[47] and held that necessity must in each case be assessed by reference to the individuals about whom information is sought:[48]

> "given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement 'necessary in a democratic society' must be interpreted in this

---

46 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [264] (emphasis added, citations omitted).

47 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [72], quoting *Klass v Germany* (App No 5029/71, 6 September 1978, Plenary Court) [42].

48 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [73] (emphasis added).

> context as requiring 'strict necessity' in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding [of] the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal."

The Court in *Szabó* also distinguished *Kennedy v United Kingdom* on the basis that the regime there[49] required individuals/premises subject to surveillance to be identified:[50]

> "in *Kennedy*, the impugned legislation did not allow for 'indiscriminate capturing of vast amounts of communications' (see *Kennedy* … § 160) which was one of the elements enabling it not to find a violation of Article 8. However, in the present case, … in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern."

54. As to the second of these requirements, reasonable suspicion:

(1) The Fourth Chamber in *Szabó* held that the surveillance approval process in the Hungarian legislation in question was incompatible with Article 8 because it did not require the authorities to demonstrate individual suspicion of the person about whom information was sought before surveillance was permitted. The Chamber held that there must be:[51]

> "a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure — and this on the basis of an individual suspicion regarding the target person (see *Roman Zakharov* … §§ 259 and 261). For the Court, only such information would allow the authorising authority to perform an appropriate proportionality test."

---

49 The United Kingdom's targeted interception provisions in RIPA s 8(1), which permitted interception of communications of "*one person as the interception subject*" or "*a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place*".

50 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [69].

51 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [71].

In particular, the Court held that Hungarian legislation allowing surveillance of persons (relevantly) "*identified … as a range of persons*" was:[52]

> "overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons 'concerned' and the prevention of any terrorist threat — let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity (see in paragraphs 72 and 73 below) with regard to the aims pursued and the means employed …"

(2) The Grand Chamber in *Zakharov* had similarly held that an authorising authority's scope of review "*must be capable of verifying the existence of a reasonable suspicion against the person concerned*",[53] indicating that such suspicion must exist whenever surveillance is ordered.

(3) The CJEU in *Watson* understood *Zakharov* in this way. It held, "*by analogy*" to *Zakharov*, that "*access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime*".[54]

54A. The decision of the Chamber in *Centrum för Rättvisa v Sweden* does not undermine this analysis. No argument to the effect of that presented above was (it seems) presented in that case,[54a] so it does not consider the point directly.[54b] Further, the regime considered bears no resemblance to those considered in *Zakharov* and *Szabó*, in particular because

---

52 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [67].

53 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [260] (emphasis added).

54 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [119].

54a See *Centrum för Rättvisa v Sweden* (App No 35252/08, 19 June 2018, Third Section) [99]–[114], which do not record any submissions of the parties on the question of "bulk" interception in general. Further, so far as Liberty is aware, there was no direct challenge by the applicant (or the intervener) to "bulk" surveillance or any submission along the lines of that set out above: see in particular the Swedish government submissions of admissibility and merits of 8 May 2015, the applicant's submissions of 31 August 2015, the further observations of the government of 19 November 2015, and the applicant's further submissions of 10 December 2015, available at the applicant's website <http://centrumforrattvisa.se/> (all of which are in English).

54b The comments in *Centrum för Rättvisa v Sweden* (App No 35252/08, 19 June 2018, Third Section) [112] in relation to "bulk" surveillance must be understood in that context.

it was "*not targeting individuals suspected of criminal conduct*".[54c] The regime in that case differs in many ways from the impugned provisions here, and is in particular narrower as to its scope and has greater safeguards.[54d] Alternatively, if *Centrum för Rättvisa* is contrary to the analysis above, it is incorrectly decided insofar as it fails to follow and apply the recent Grand Chamber decision in *Zakharov* (as applied in *Szabó* and set out immediately above).[54e]

Foreseeability/necessity — Safeguards/necessity in a democratic society

55. In addition to the mandatory requirements mentioned above, secret surveillance regimes must, as a "*minimum safeguard*" to avoid abuse, set out:[55]

> "the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the

---

[54c] *Centrum för Rättvisa v Sweden* (App No 35252/08, 19 June 2018, Third Section) [130].

[54d] In particular, the regime was limited to surveillance in support of foreign, defence and security policy and to identify threats to the country, with surveillance for the purpose of law enforcement or prevention of crime expressly prohibited (at [8]), there were eight enumerated purposes for which signals could be collected (including surveying external military threats, development and proliferation of weapons of mass destruction, strategic circumstances concerning international terrorism and other serious cross-border crime threatening essential national interests, and foreign conflicts), a specific natural person could not be targeted (at [9]), surveillance operation as well as the search terms or categories of search terms to be used had to be defined in a specific application and authorised in advance by a Court (at [18]), for surveillance to be authorised its value had to be "*clearly greater than the possible interference with personal integrity*" (at [19]), it was prohibited altogether to intercept communications between persons in Sweden (and if such communications were intercepted they had to be destroyed immediately upon the domestic nature becoming apparent) (at [15], [26]), intercepted material had to be destroyed immediately if it concerns a specific natural person and lacks intelligence importance, or was protected by constitutional provisions on media sources, or contained information shared between an attorney and their client, or involved information given in a religious context unless there are exceptional reasons (at [25]), any personal data retained had to be destroyed within one year of collection (at [31]), and if search terms directly related to a specific individual were used, that person had to be notified once this was operationally possible (although the notification obligation ceased if notification was not possible within one year) (at [44]–[45]).

[54e] In that regard, in commenting on "*bulk interception regimes*" at [112], *Centrum för Rättvisa v Sweden* (App No 35252/08, 19 June 2018, Third Section) does not seek to reconcile its comments with the statement in *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [69] (set out in paragraph 53(2) above) that legislation that enabled "*strategic, large-scale interception*" was "*a matter of serious concern*".

[55] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [231] (citations omitted) (emphasis added). The same requirements are repeated in: *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [56]; *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [95]. See also *Huvig v France* (App No 11105/84, 24 April 1990, Chamber) [34]; *Kruslin v France* (App No 11801/85, 24 April 1990, Chamber) [35]; *Valenzuela Contreras v Spain* (App No 58/1997/842/1048, 30 July 1998, Judgment) [46(iv)].

precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed …"

56. Also relevant are *ex post* means of reviewing the lawfulness of surveillance under domestic law, in particular any notification to the individual monitored and any ability to seek a remedy before domestic courts.[56]

57. These matters that must be set out with sufficient detail and clarity in a surveillance law to ensure its compatibility with Articles 8 and 10 are referred to as "**critical features**" below.

58. Further, in the context of surveillance laws, the ECtHR typically does not assess separately whether a law is sufficiently clear and detailed as to the critical features and whether it is necessary in a democratic society. These matters are taken together in recent decisions.[57] However, the case-law establishes that a secret surveillance regime must:

    (1) Have sufficient clarity and detail on each critical feature, as each of these is one of the "*conditions necessary*" for compliance with Articles 8(2) and 10(2);[58] and

    (2) Additionally, have sufficient clarity and detail overall, considering the operation of its provisions together.

58A. Contrary to the assertion in SGR ¶42, the assessment of necessity in this context does **not** require or entail examination of "*the actual exercise of the powers concerned*". The cases referred to in these Grounds consider the sufficiency of the legal framework **without regard** to particular exercises of the power, when considering both whether the regime is "in accordance with the law" and whether it is "necessary in a democratic society".

---

[56] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [234], [298]; *Dragojević v Croatia* (App No 68955/11, 15 January 2015, First Section) [99]–[100]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [56].

[57] See, eg, *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [236], [302], [304]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [58], [89].

[58] *Valenzuela Contreras v Spain* (App No 58/1997/842/1048, 30 July 1998, Judgment) [59]. See, eg, *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App No 62540/00, 30 January 2008, Fifth Section) [78]–[84] (substantial compliance as to some critical features), [85]–[93] (failure to provide procedure for examination, storage and use, precautions when communicating the data, and circumstances of erasure and destruction); *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [266].

59. *Zakharov* and *Szabó*, which review previous ECtHR cases (including *Weber and Saravia v Germany*)[59] and distil the applicable principles, offer the following guidance in assessing whether a secret surveillance law provides effective safeguards on each of the critical features with sufficient certainty and detail:

(1) **Scope of application:** Offences or grounds which may give rise to interception need not be stated exhaustively but must be "*sufficiently clear*".[60] Discretion is likely too broad where: (i) surveillance can be ordered for a "*wide range*" of offences or grounds;[61] and/or (ii) there is no connection required between the offence or ground for surveillance and the person whose communications are intercepted or any connection is distant.[62]

(2) **Duration:** Domestic law may leave the overall duration of a warrant to executive discretion so long as it indicates "*the period after which an interception warrant will expire, the conditions upon which a warrant can be renewed and the circumstances in which it must be cancelled*".[63] Failure to require surveillance to cease where no longer necessary is likely to indicate insufficient safeguards on duration.[64]

(3) **Authorisation procedure:** The authorisation procedure must be "*capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration*".[65] The elements of this procedure that must be stated clearly and in detail include:

(a) the "*authority competent to authorise the surveillance*", which must be "*sufficiently independent from the executive*" or subject to control by an independent body;[66]

---

59 *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section).

60 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [244].

61 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [244], [246].

62 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [245], [248].

63 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [250].

64 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [252].

65 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [257].

66 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [258].

(b) that authority's "*scope of review*", which must include the verification of the existence of a reasonable suspicion (see paragraph 52(2) above) and whether the requested interception is necessary and proportionate — the reviewing authority should, in general, be provided with all the material before the initial decision-maker;[67]

(c) the "*content of the interception authorisation*", which must identify a person or the premises to be placed under surveillance;[68] and

(d) any urgency procedure, which must provide "*sufficient safeguards to ensure that it is used sparingly and only in duly justified cases*", in particular by defining urgency so as to avoid conferring "*an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure*" (for example, by requiring an "*immediate risk*")[69] and ensuring review of "*whether the use of the urgent procedure was justified*" and what should be done with material obtained.[70]

(4) **Procedure for use/examination/storage and precautions when communicating:** The procedures governing storage, use and communication of intercept data should enable the state to "*minimise the risk of unauthorised access or disclosure*".[71] An obligation to keep records of interceptions is "*particularly important*".[72] A supervisory body (preferably a judge) should supervise the storage of, access to, use of, processing of, communication of and destruction of the intercepted content and be "*vested with sufficient powers*" to ensure that prescribed procedures are followed.[73] Powers and the publicity of actions to remedy any

---

67 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [260]–[261].

68 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [257], [264]–[265].

69 As in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App No 62540/00, 30 January 2008, Fifth Section) [16], [82], a requirement that was held to be compatible with the Convention in *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [266].

70 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [266].

71 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [253].

72 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [272].

73 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [273]–[275].

breach/illegality are important.[74] The government must demonstrate the "*practical effectiveness*" of supervision arrangements with "*appropriate examples*".[75]

(5) **Circumstances of destruction:** "*The automatic storage of clearly irrelevant data cannot be considered justified under Article 8.*"[76] An "*unlimited discretion*" to store data, even only in some circumstances, is unlikely to give a "*sufficiently clear*" indication of when data may be retained.[77]

(6) **Notification:** "*As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should … be provided to the persons concerned*".[78] Alternatively, as in *Kennedy v United Kingdom*, any person who "*suspected that his communications were being or had been intercepted*" must be able to have its legality examined without any need for "*notification to the interception subject that there had been an interception of his or her communications*".[79]

(7) **Remedies:** The circumstances in which a person is notified of surveillance, any mechanism to ascertain whether surveillance has occurred (and the effectiveness of that mechanism), and the remedies under national law to test the legality of surveillance are relevant.[80] Where the effectiveness of domestic remedies depends on an individual's knowledge of surveillance, the absence of a requirement to notify the person of surveillance when appropriate is "*incompatible with the Convention*".[81]

60. *Zakharov* and *Szabó* have considered interception of voice and other electronic communications, for which the strict foreseeability requirements are onerous. The same requirements apply to communications data.[82] However, for interferences of greater

---

74 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [282]–[283].
75 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [284].
76 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [255].
77 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [256].
78 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [287].
79 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [287]–[288].
80 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [289]–[292].
81 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [288], [298].
82 *Liberty v GCHQ (No 1)* [2014] UKIPTrib 13_77-H [114] (Burton J).

seriousness and intensity, the foreseeability requirements are even more demanding — that is, the level of clarity, detail and effectiveness of the surveillance regime in constraining executive discretion that the ECHR requires are greater again.[83] Thus, for equipment interference — which permits access to an even wider range of information and is not limited to its transmission or storage in a telecommunications system — the foreseeability requirements must be applied with greater strictness.

61. ~~No c~~Codes of practice have~~, so far as Liberty is aware,~~ been made under Schedule 7 of the Act for each of the impugned provisions except for Part 4 ~~(or otherwise)~~.[~~84~~] The SGR do not address the content of any of the codes of practice (because they were submitted before the codes of practice were made). However, should the Defendants ~~(1) publish final codes of practice and (2)~~ seek to argue that any published code of practice increases the certainty or detail of relevant provisions of the Act:

(1) a code of practice can be modified without express parliamentary approval under Schedule 7 para 5;[84a]

(2) a person's failure to comply with a Code "*does not of itself make that person liable to criminal or civil proceedings*" under Schedule 7 para 6(2); and

(3) an authority exercising powers under the Act may "*depart* [from a code] ... *if it has cogent reasons for doing so*"[85] but, conversely, a code of practice cannot validly fetter the exercise of statutory discretion — an authority must consider departing from a code of practice if asked to do so.[86]

---

83 See *RE v United Kingdom* (App No 62498/11, 27 October 2015, Fourth Section) [130], in the context of physical surveillance, holding that the decisive factor in determining the strictness of foreseeability requirements is "*the level of interference with an individual's right to respect for his or her private life*".

~~84 See above n 17 on the recently published draft codes of practice.~~

84a Where a code of practice is modified, either the revised draft code must be laid before and approved by resolution of Parliament or the regulations giving force to the revised code (and the code) must be laid before Parliament: Schedule 7 para 5(5). In the latter case, it is sufficient that the code is laid before Parliament. There is no requirement for approval by resolution. This is in distinction to the power to make a new code under Schedule 7 para 4(4), which requires express parliamentary approval by resolution of all regulations making a code.

85 *R (Munjaz) v Mersey Care NHS Trust* [2005] UKHL 58, [2006] 2 AC 148 [21] (Lord Bingham), [69] (Lord Hope).

86 *R (Sandiford) v Secretary of State for Foreign and Commonwealth Affairs* [2014] UKSC 44, [2014] 1 WLR 2697 [54] (Lord Carnwath and Lord Mance), [81], [83] (Lord Sumption).

62. The critical factors are likely to be considered again by the ECtHR in the pending cases of *10 Human Rights Organisations v United Kingdom*,[87] ~~and~~ *Big Brother Watch v United Kingdom*,[88] and *Bureau of Investigative Journalism v United Kingdom*,[88a] which challenge the compatibility with Article 8 and/or Article 10 of RIPA s 8(4), a similar (but narrower) provision to those for bulk interception warrants under Part 6 Chapter 1~~2~~.

Foreseeability/necessity — Retention (Part 7)

63. Insofar as Part 7 constitutes part of the regime for retention of and access to communications and other information obtained under the Act, the strict foreseeability requirements apply to it as part of a secret surveillance regime.

64. In addition, the same strict foreseeability requirements apply to Part 7 considered as a freestanding regime for government collection of data concerning individuals,[89] as the ECtHR said in *S and Marper v United Kingdom*:[90]

> "[The Court] reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness …"

(2) Articles 8 and 10 ECHR and journalistic sources

65. Articles 8 and 10 ECHR require particular safeguards where journalistic sources are subject to interception.

---

87 App No 24960/15, communicated to the United Kingdom on 24 November 2015.

88 App No 58170/13, communicated to the United Kingdom on 9 January 2014.

88a App No 62322/14, communicated to the United Kingdom on 5 January 2015.

89 *R (T) v Chief Constable of Greater Manchester Police* [2014] UKSC 35 [111], [114] (Lord Reid), quoting and applying *MM v United Kingdom* (App No 24029/07, 13 November 2012, Fourth Section) [206]–[207].

90 *S and Marper v United Kingdom* (App Nos 30562/04 and 30566/04, 4 December 2008, Grand Chamber) [99] (emphasis added), citing (amongst other cases) *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section), *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (App No 62540/00, 30 January 2008, Fifth Section) [75]–[77], and *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [62]–[63].

(a) Interference

66. ECtHR case-law establishes that the existence of secret surveillance legislation that permits the state to obtain a journalist's confidential sources is "*in itself ... an interference*" with a journalist's right to freedom of expression, whether indiscriminate or targeted.[91] This is because "*a chilling effect will arise wherever journalists are seen to assist in the identification of anonymous sources*".[92] Interference arises through requiring a journalist to provide, or the state obtaining, "*information identifying a source*" (which is "*any person who provides information to a journalist*"), including both the fact of acquisition of information and the unpublished content.[93] The interference arises both under Article 8 and Article 10.[94]

(b) Mandatory requirements for journalistic materials

67. Where powers are, or may be, directed at journalists or it is intended or possible that journalistic sources will be revealed by the surveillance/interception, Articles 8(2) and 10(2) require that, to be "in accordance with the law" and "prescribed by law", in addition to satisfying the strict foreseeability requirements described above, the regime must:

    (1) "[G]*uarantee ... review* [of the interception decision] *by a judge or other <u>independent and impartial</u> decision-making body*" with power to issue, reject or qualify the decision to intercept;[95]

    (2) Provide for this review <u>before</u> interception occurs or, in urgent cases, <u>before</u> any use is made of the information obtained (which requires that the independent body

---

91 *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [144]–[146]; *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [88].

92 *Nagla v Latvia* (App No 72469/10, 16 July 2013, Fourth Section) [82].

93 *Nagla v Latvia* (App No 72469/10, 16 July 2013, Fourth Section) [81]; *Sanoma Uitgfevers BV v Netherlands* (App No 38224/03, 14 September 2010, Grand Chamber) [64].

94 *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [89], [102].

95 *Sanoma Uitgfevers BV v Netherlands* (App No 38224/03, 14 September 2010, Grand Chamber) [90], [97] (emphasis added); *Nagla v Latvia* (App No 72469/10, 16 July 2013, Fourth Section) [87]; *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [100]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [77].

in urgent cases has the power to prevent use even after journalistic materials have been intercepted);[96] and

(3) Require the independent body to consider "*whether the interest of the criminal investigation overrode the public interest in the protection of journalistic sources*",[97] bearing in mind that "*limitations on the confidentiality of journalistic sources call for the most careful scrutiny by the Court*" and that there must be an overriding public interest to require a journalistic source to be revealed.[98]

68. Where powers are not, or cannot be, directed at journalists or used to identify journalistic sources, Articles 8(2) and 10(2) require that safeguards restrict the use of material obtained such that "*the disclosure of journalistic sources* [is kept to] *to an unavoidable minimum*".[99]

(3) Articles 8 and 10 ECHR and communications between lawyers and clients

69. Articles 8 and 10 ECHR require particular safeguards where a client's communications with their lawyer, including legally privileged materials, are subject to interception.

(a) Interference

70. Article 8 affords "*strengthened protection*" to the making and content of communications between lawyers and their clients[100] ("**lawyer–client communications**"), regardless of whether they are technically covered by legal privilege under national law. The ECtHR stated in *Michaud v France* that:[101]

---

96 *Sanoma Uitgfevers BV v Netherlands* (App No 38224/03, 14 September 2010, Grand Chamber) [91], [99].

97 *Sanoma Uitgfevers BV v Netherlands* (App No 38224/03, 14 September 2010, Grand Chamber) [100]; *Nagla v Latvia* (App No 72469/10, 16 July 2013, Fourth Section) [88].

98 *Nagla v Latvia* (App No 72469/10, 16 July 2013, Fourth Section) [95], [97] (emphasis added); *News Group Newspapers Ltd v Commissioner of Police of the Metropolis* [2015] UKIPTrib 14176-H [100], [104], [106]–[107] (Burton J).

99 *Telegraff Media Nederland Landelijke Media BV v Netherlands* (App No 39315/06, 22 November 2012, Third Section) [96], approving *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [152].

100 *RE v United Kingdom* (App No 62498/11, 27 October 2015, Fourth Section) [131]; *Michaud v France* (App No 12323/11, 6 December 2012) [118]. This is implicit in the government's concession in *Belhadj v Security Service* [2015] UKIPTrib 13_132-H [2] (Burton J) that the "*the regime for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material*" under RIPA and the relevant Code of Practice was not in accordance with the law under Article 8(2).

101 *Michaud v France* (App No 12323/11, 6 December 2012, Fifth Section) [117] (emphasis added).

"by virtue of Article 8, correspondence between a lawyer and his client, whatever its purpose (strictly professional correspondence included …), enjoys privileged status where confidentiality is concerned … (… this applies, as mentioned earlier, to all forms of exchanges between lawyers and their clients) …"

(b) Mandatory requirements for confidential legal materials

71. The ECtHR's case-law establishes that legislation that authorises "*the surveillance of privileged communications*" (and other lawyer–client communications) must contain specific provisions directed to those communications which set out "*clear and stringent rules governing the authorisation, circumstances, manner, and control over the fruits, of any such surveillance*".[102] At a minimum, those are:

(1) clear rules about "*how, under what conditions and by whom the distinction is to be drawn between*" lawyer–client communications and others — that is, a clear legal rule and framework for determining which communications receive strengthened protection;[103]

(2) a decision about whether information is a lawyer–client communication by (or supervised by) someone who is not "*a member of the executive*", such as an independent body or someone under "*supervision by an independent judge*";[104]

(3) an assessment of whether a communication is protected before surveillance commences or, at least, before any use a communication is made;[105] and

(4) a requirement that the interest of lawyer–client confidence receives "*particular weight*" when the necessity/proportionality of the interception and/or use of the lawyer–client communication are considered.[106]

---

102 *McE v Prison Service of Northern Ireland* [2009] UKHL 15; [2009] 1 AC 908 [111] (Lord Neuberger); see also [41] (Lord Phillips); *RE v United Kingdom* (App No 62498/11, 27 October 2015, Fourth Section) [97], [115], [131]; *Michaud v France* (App No 12323/11, 6 December 2012, Fifth Section) [130].

103 *Kopp v Switzerland* (App No 13/1997/797/1000, 25 March 1998, Judgment) [73]; see also at [74]–[75].

104 *Kopp v Switzerland* (App No 13/1997/797/1000, 25 March 1998, Judgment) [74].

105 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [77], where the Court refers to *Kopp* as "*circumstances necessitating ex ante authorisation*".

106 *Michaud v France* (App No 12323/11, 6 December 2012, Fifth Section) [117].

71A. In their Skeleton Argument of 19 February 2018 at ¶¶104–107 ("**D Pt 4 Skel**"), the Defendants mischaracterise Liberty's case as set out immediately above and advance various contentions about the effect of the cases to which Liberty has referred. Liberty maintains that the effect of the ECtHR's case law is correctly set out in paragraph 70 above. It responds to the Defendants' submissions as follows:

(1) The Defendants' main contention (D Pt 4 Skel ¶¶104, 107) is that *Michaud v France*, *McE v Prison Service of Northern Ireland*, *RE v United Kingdom*, *Kopp v Switzerland* and *Szabó* do not identify particular requirements that secret surveillance regimes must contain (under Articles 8 and 10 ECHR) relating to all lawyer–client communications. This is wrong. It is contrary to clear statements in each of those cases (such as that from *Michaud* set out in paragraph 70 above), which reflect the increased sensitivity and expectation of confidence that attaches to lawyer–client communications.[106a]

[106a] *McE v Prison Service of Northern Ireland* [2009] UKHL 15; [2009] 1 AC 908 [111] (Lord Neuberger):
"*none of these problems can call into question the lawfulness of the statutory authorising of the surveillance of privileged communications, although they underline the fundamental requirement of clear and stringent rules governing the authorisation, circumstances, manner, and control over the fruits, of any such surveillance*".
Michaud v France (App No 12323/11, 6 December 2012, Fifth Section) [118]–[119]:
"*The result is that while Article 8 protects the confidentiality of all 'correspondence' between individuals, it affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, that is at stake. Indirectly but necessarily dependent thereupon is the right of everyone to a fair trial, including the right of accused persons not to incriminate themselves.*
This additional protection conferred by Article 8 on the confidentiality of lawyer-client relations, and the grounds on which it is based, lead the Court to find that, from this perspective, legal professional privilege, while primarily imposing certain obligations on lawyers, is specifically protected by that Article."
RE v United Kingdom (App No 62498/11, 27 October 2015, Fourth Section) [131]:
"*The present case concerns the surveillance of legal consultations taking place in a police station, which the Court considers to be analogous to the interception of a telephone call between a lawyer and client. The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential (Michaud v France, no 12323/11, § 118, ECHR 2012). The Court therefore considers that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person's right to respect for his or her private life and correspondence; higher than the degree of intrusion in Uzun and even in Bykov. Consequently, in such cases it will expect the same safeguards to be in place to protect individuals from arbitrary interference with their Article 8 rights as it has required in cases concerning the interception of communications, at least insofar as those principles can be applied to the form of surveillance in question.*"

(2) Liberty does **not** contend, contrary to the suggestion in D Pt 4 Skel ¶105, that the application of the particular requirements identified above turns on whether communications are classified as privileged under domestic law. *Michaud*, which considers secret surveillance cases including *Kopp* (where a lawyer's telephones were tapped), establishes that these protections are required to be afforded to all lawyer–client communications, as explained in paragraph 70 above.

(3) D Pt 4 Skel ¶¶106(e) and 107 rightly accept that *Michaud* establishes that Article 8 confers "*strengthened protection*" for lawyer-client exchanges. The Defendants correctly do not dispute that this applies in the context of surveillance regimes.[106b] *RE v United Kingdom* reiterates this, and explains that it applies in the context of interception of lawyer–client communications (see footnote [106a] above). Further, the Defendants do not dispute that this means that a surveillance regime must ensure that, in considering necessity/proportionality, the expectation of confidence in such communications must receive particular weight (see paragraph 71(4) above).

(4) The suggestion in D Pt 4 Skel ¶106(c) that *Kopp* does not establish some of the safeguards that are required where lawyer–client communications are intercepted is incorrect. *Kopp* states:[106c]

> "…Even though the [Swiss] case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the [surveillance] law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters

---

Kopp v Switzerland (App No 13/1997/797/1000, 25 March 1998, Judgment) [72], [75] (emphasis added):
"*tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly 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 use is continually becoming more sophisticated …*
In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. Consequently, Mr Kopp, ***as a lawyer,*** *did not enjoy the minimum degree of protection required by the rule of law in a democratic society.*"
Szabó and Vissy v Hungary (App No 37138/14, 12 January 2016, Fourth Section) [77], set out in paragraph [71A(5)] below.

[106b] If D Pt 4 Skel ¶107 seeks to suggest that this protection does not attach to all lawyer client exchanges, it is wrong: see paragraph [71A(2)] above.

[106c] *Kopp v Switzerland* (App No 13/1997/797/1000, 25 March 1998, Judgment) [73]–[74].

specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel.

Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence."

Kopp therefore makes clear that, where lawyer–client communications are subject to secret surveillance, the surveillance law contains sufficient safeguards where it:

(a) States clearly how (by what rules), under what conditions and by whom material that is a lawyer–client communication (material that relates to the lawyer's professional work) is to be identified (as set out in paragraph 71(1) above); and

(b) Provides for someone independent of the executive, or with supervision from someone who is independent of the executive, to determine whether a communication is a lawyer–client communication (as set out in paragraph 71(2) above).

(5) Contrary to the unreasoned assertion in D Pt 4 Skel ¶106(d), the reference in *Szabó* to *Kopp* as a situation where there are "*circumstances necessitating ex ante authorisation*" was a "*general observation*" about cases where lawyer–client communications are intercepted. The Court said:[106d]

"Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny (see *Klass* ... §§ 42 and 55). The *ex ante* authorisation of such a measure is not an absolute requirement per se, because where there is extensive post factum judicial oversight, this may counterbalance the shortcomings of the authorisation (see *Kennedy* … § 167). **Indeed, in certain respects and for certain circumstances, the Court has found already that ex ante (quasi-)judicial authorisation is necessary, for example in regard to secret surveillance measures targeting the media.** In that connection the Court held that a post factum review cannot restore the confidentiality

[106d] *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [77] (emphasis added).

of journalistic sources once it is destroyed (see *Telegraaf Media Nederland Landelijke Media BV and Others v the Netherlands*, no 39315/06, § 101, 22 November 2012; **for other circumstances necessitating *ex ante* authorisation see *Kopp v Switzerland***, 25 March 1998, Reports 1998 II)."

The Court indicates, by the reference to *Kopp*, that the requirements in relation to interception of communications of journalists (set out in paragraph 67 above) and those of lawyers are analogous. The concern in *Kopp*, as set out in paragraph [71A(4)] above, was the lack of clear and effective safeguards for lawyer–client communications. In saying that interception of lawyer–client communications requires *ex ante* authorisation, *Szabó* indicates that lawyer–client communications require judicial authorisation before interception (or, in urgent cases, use of intercepted material), in the same way as the cases concerning journalistic sources (as set out in paragraph 71(3) above). D Pt 4 Skel ¶106(d) does not attempt to identify any circumstance peculiar to *Kopp* that required *ex ante* authorisation (so as to explain away the ECtHR's holding), and no such circumstance is apparent.

(3A) Article 14 ECHR and nationality/national origin/United Kingdom residency

71B. For the reasons set out below, certain safeguards in Chapter 6 Part 1 and Chapter 6 Part 3, which apply only where a person is known to be physically present in the United Kingdom, discriminate contrary to Article 14 ECHR in an unjustifiable manner. These provisions are incompatible with the ECHR on this further basis.

71C. Article 14 ECHR states:

"The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

71D. It is well established that the following questions arise under Article 14:[106e]

"(1) Do the facts fall within the ambit of one or more of the Convention rights? (2) Was there a difference in treatment in respect of that right between the complainant and others put

[106e] *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 AC 68 [50] (Lord Bingham).

forward for comparison? (3) If so, was the difference in treatment on one or more of the proscribed grounds under article 14? (4) Were those others in an analogous situation? (5) Was the difference in treatment objectively justifiable in the sense that it had a legitimate aim and bore a reasonable relationship of proportionality to that aim?"

(a) Secret surveillance regimes fall within the ambit of convention rights

71E. As explained in paragraphs 34–39 above, it is well-established that the existence of secret surveillance regimes, and each of the interception, retention, examination and use of retained information, interfere with the rights protected by Articles 8 and 10 ECHR. Accordingly, the impugned provisions fall within the ambit of these Convention rights.

(b) Difference in treatment of relevant individuals on Convention-prohibited grounds

71F. Article 14 prohibits discrimination in the enjoyment of rights under Articles 8 and 10 ECHR on grounds including national origin and nationality[106f] and other status, namely, residence in the United Kingdom.[106g]

71G. As explained below in paragraphs 119B–119E and 149B–149E, the bulk interception power (Chapter 6 Part 1) and bulk equipment interference power (Chapter 6 Part 3) contain different safeguards for the "selection for examination" of intercepted or hacked material depending on whether or not a person is known to be in the British Islands at the time when the "selection for examination" is carried out. Accordingly, there is a difference in treatment between those persons known to be, and those not known to be, in the British Islands.

71H. As matters of fact:

(1) A British person is substantially more likely to be present in the British Islands than a person who is a non-British person.

(2) A person of British national origin is substantially more likely to be present in the British Islands than a person who is not of British national origin.

[106f] See, eg, *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 AC 68 [49]–[50] (Lord Bingham).

[106g] See, eg, *Carson v United Kingdom* (App No 42184/05, 16 March 2010, Grand Chamber) [70].

(3) A person who is resident in the United Kingdom is substantially more likely to be present in the British Islands than a person who is not resident in the United Kingdom.

71I. The application of different safeguards depending on whether or not a person is present in the United Kingdom where intercepted or otherwise obtained material is "selected for examination" discriminates indirectly on the basis of nationality and/or national origin and/or "other status" (residency in the United Kingdom), since the safeguards and restrictions under those provisions:

(1) Are substantially less likely to be enjoyed by non-British nationals than by British nationals;

(2) Are substantially less likely to be enjoyed by persons not of British origin than by persons of British origin; and/or

(3) Are substantially less likely to be enjoyed by persons not resident in the United Kingdom than by persons who are resident in the United Kingdom.

71J. It is not the case (as the Defendants may submit) that the difference in treatment results solely from current location and not the nationality, national origin and/or residency of such persons. This is not a case of "*regional differences of treatment, resulting from the application of different legislation depending on the geographical location of an applicant*",[106h] but instead "*the different application of the same ... legislation to persons depending on their residence and presence abroad*".[106i]

71K. Those who are British nationals, of British origin or resident in the United Kingdom, and those who are not, are analogous and/or relevantly similar in relation to their electronic communications and electronically stored information. There is no relevant difference in their characteristics.[106j] They are appropriate comparators.

[106h] This is how the ECtHR explained *Magee v United Kingdom* (App No 28135/95, 6 June 2000, Third Section) [50] in *Carson v United Kingdom* (App No 42184/05, 16 March 2010, Grand Chamber) [70].

[106i] *Carson v United Kingdom* (App No 42184/05, 16 March 2010, Grand Chamber) [70].

[106j] On this issue, see, eg, *A v Secretary of State for the Home Department* [2004] UKHL 56, [2005] 2 AC 68 [53] (Lord Bingham).

(c) No justification

71L. It is in those circumstances for the Defendants to advance any justification for the difference in treatment between British nationals, those of British national origin and United Kingdom residents and those who do not have these characteristics. Should the Defendants seek to advance any justification, Liberty may seek to respond either by submissions or evidence as appropriate, including before permission is given.

71M. Nonetheless, Liberty notes for completeness that, if the Defendants contend that they have greater power to investigate persons within than those outside the United Kingdom, this would provide no justification.[106k] It does not follow that lesser safeguards should apply when a factor referable to an individual not known to in the United Kingdom is used to "select for examination" material that has been intercepted or hacked under Chapter 6 Part 1 or Chapter 6 Part 3 of the Act. Once such a factor has been identified and will be used to "select for examination" material collected under those provisions:

(1) It is possible to obtain an approval directed to that individual, by reference to the factor in question, even if their full identity and location is not known.

(2) It is irrelevant that other powers might in theory be able to be used to investigate the person to whom the factor is referable. Where the powers under the Act are used, the existence of other powers (that are *ex hypothesi* not being used or have been exhausted) does not reduce the need for safeguards for the powers under the Act.

71N. The distinction drawn by these safeguards under Chapter 6 Part 1 and Chapter 6 Part 3 of the Act is arbitrary. The applicability of the safeguards depends on whether it is **known** that a person is present somewhere in the British Islands. As soon as a person leaves the British Islands, the United Kingdom authorities are free to select for examination any material that is referable to that particular person. As a result:

[106k] *Liberty v Secretary of State for the Foreign and Commonwealth Office* [2014] UKIPTrib 13_77-H [147] (Burton J) appeared to accept that discrimination based on national origin was effected by similar provisions in RIPA to those Liberty challenges here on this basis. To the extent that at [148] the IPT held that such discrimination was justified: (1) any justification here will turn on the arguments and evidence in these proceedings, so that finding cannot be automatically applied to Part 6 Chapter 1 and Part 6 Chapter 3; and (2) alternatively, it was wrong and should not be followed.

(1) If the United Kingdom authorities wish to select for examination intercepted or hacked material using the name of an employee of Liberty who they know is about to board a flight from London to Paris, they must obtain ministerial authorisation and the authorisation of a Judicial Commissioner to do so (by obtaining a targeted examination warrant under Chapter 2 or Chapter 5). However, if the United Kingdom authorities wish to select material for examination using the name of the same employee of Liberty when that person is about to board a flight from Paris to London, there is no such requirement. The position is then inverted when the person reaches their destination. There is no logical reason for providing different levels of protection in these two situations.

(2) Similarly, if United Kingdom authorities wish to target an NGO's London office (using factors referable to people at that office) they would need a targeted examination warrant. But if they wish to target the same NGO's German office to obtain the communications of one of its London staff members abroad (or use factors referable to people in that office in order to obtain the communications of one of its London staff members), they would not need to do so. Again, this distinction lacks any rational basis.

(3) The extent of the United Kingdom authorities' knowledge about the whereabouts of a person of interest does not necessarily bear any correlation to the applicability of the safeguards. For example, even if the United Kingdom authorities know the exact location of a person in a foreign country and have placed that person under direct visual surveillance, they may nevertheless select for examination intercepted material referable to that person without according the safeguard of specific ministerial and Judicial Commissioner approval. By contrast, if the United Kingdom authorities merely know that a person is somewhere in the British Islands, but have no idea exactly where, they are precluded from selecting for examination material using factors referable to that person unless they obtain a targeted examination warrant. It may be much easier for the United Kingdom authorities to investigate the former, yet that person enjoys significantly less protection than the latter.

(4) Victim status for the purposes of the Human Rights Act

72. As Liberty and its staff members may in the course of their employment be subject to the measures and discrimination which it seeks to challenge, Liberty (and its staff) are "victims" of the measures and discrimination for the purposes of a challenge under the Human Rights Act 1998. Liberty's standing and victim status were not challenged in the cases referred to above which it brought in its own name. Nor have the Defendants suggested that Liberty is not a victim.

(5) EU law

73. The impugned provisions are within the material scope of EU law and therefore subject to the constraints it imposes, as to quality of law and substantially. Liberty explains each of these below.

73A. To the extent that any of the impugned provisions are incompatible with EU law, they do not comply with domestic law (for the purposes of the ECHR) and, for that additional reason, they are "not in accordance with the law" and not "prescribed by law" under ECHR Articles 8 and 10: *Big Brother Watch v United Kingdom* (App No 58170/17 et al, 18 September 2018, First Section) [465]–[468].

(a) Material scope of EU law

Principles

74. The CJEU's decisions in *Watson*, *PI* and *La Quadrature* confirms that national legislative measures (i) requiring communications service providers to retain communications data and/or provide communications data to national authorities and/or (ii) relating to the access to such data by national authorities are within the scope of Directive 2002/58/EC[107] ("**Directive 2002/58**", the "**e-Privacy Directive**")[108] and therefore within the material scope of EU law.

---

[107] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.

[108] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [75]–[76].

75. Directive 2002/58/EC by Article 3 applies to the processing of data in connection with public telecommunications systems. By Article 1(3), it does not apply to "*activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law*". Article 15(1) of Directive 2002/58[109] states:

> "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

76. When Articles 1(3) and 15(1) are read together, it is apparent that some activities that might concern public security, defence, State security (including economic well-being) and State activities in criminal law are nonetheless within the scope of the Directive insofar as they involve processing of data in connection with telecommunications systems. That is, Article 15(1) makes clear that, just because a measure pursues the purpose of public security, defence, etc, mentioned in Article 1(3), this does not of itself mean that activity falls outside the material scope of EU law. The decisions in *PI* (at [29]–[30], [32], [39], [48]–[49] and the conclusion as to Telecommunications Act 1984 s 94) and *La Quadrature* (at [87]–[104]) make the contrary unarguable.

77. That is logical and necessary to prevent the rights protected under Directive 2002/58[110] from becoming nugatory: a national measure may pursue multiple purposes or objects,

---

[109] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (as amended) (the "**Data Protection Directive**") is also relevant, but has materially identical application and exclusion provisions.

[110] Article 5(1) requires Member States to "*ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services*" and, in particular, to "*prohibit listening, tapping, storage or other kinds of interception or*

and it would render the rights under Directive 2002/58 virtually at nought if a national measure fell outside the scope of Directive 2002/58 merely because it concerns public security, defence, etc. Thus, as the CJEU said in *Watson*, it is not the case that "*the legislative measures referred to in Article 15(1) of Directive 2002/58 are excluded from the scope of that directive*" due to the "*general structure*" of Directive 2002/58.[111] Instead:[112]

> "Article 15(1) necessarily presupposes that the national measures referred to therein, such as those relating to the retention of data for the purpose of combating crime, fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met."

78. As the CJEU held in *Watson*, where national measures enable the Member State to impose obligations upon third parties, such as telecommunications providers, that necessarily involve the processing of personal data, the national measure falls within the material scope of EU law.[113] That is further affirmed in *PI* at [48]–[49].

79. Further, national measures that pursue the purposes in Article 15(1) fall within the material scope of EU law to the extent that they:

    (1) Require providers of electronic communications services, for the purposes in Article 15(1), to grant national authorities access to personal data retained by them or requires the retention of data so that it is available to national authorities;[114]

---

surveillance of communications and the related traffic data by persons other than users, without the consent of the users involved, except when legally authorised to do so in accordance with Article 15(1)". Article 5(3) requires Member States to ensure that the storing of or gaining access to information stored in the terminal equipment of a subscriber/user "*is allowed only on condition that the scriber or user concerned has given his or her consent*". Article 6(1) requires that traffic data relating to subscribers/users is "*erased or made anonymous when it is no longer needed for the purpose of transmission of a communication*", subject to presently immaterial exceptions. Article 9(1) requires location data (other than traffic data) relating to users /subscribers to be processed "*only … when they are made anonymous, or with the consent of the users or subscribers*" for a value added service.

111 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [73].

112 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [73].

113 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [75].

114 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [78]–[79].

(2) Depend in practice on the cooperation of communications service providers ("**CSP**s"), and involve the processing of personal data by a cooperating CSP (for example, by transferring it to the government);[115] ~~and/or~~

(3) "[G]*overn … the activity of providers of electronic communications services*";[116] and/or

(4) Provide for and/or regulate the retention and/or use and/or other processing by the state of any data provided to it in circumstances that fall within the material scope of EU law (regardless of the use made of it): *PI* at [56].

The impugned provisions are within the material scope of EU law

80. The impugned provisions of the Act all fall within the material scope of EU law.

81. *Watson* held that "*national legislation, such as that at issue in the main proceedings in Cases C-203/15 and C-698/15* [that is, *Watson*]*, falls within the scope of Directive 2002/58*".[117] The CJEU had earlier set out the relevant legislation, namely, the power under DRIPA to issue a retention notice and the power under RIPA s 22 to access the retained data.[118]

82. The powers at issue in *Watson* are indistinguishable for this purpose from those in Part 4 of the Act. Part 4 re-enacts DRIPA and RIPA s 22. Accordingly, Part 4 is within the material scope of EU law.

83. Further, there is no relevant distinction for the purposes of the application of EU law between the power to issue bulk acquisition warrants under Part 6 Chapter 2 and Part 4: the purposes for which the latter may be issued are included within the purposes of Part 4 (and RIPA s 22, considered in *Watson*); ~~and~~ bulk acquisition warrants similarly work by imposing obligations upon third party telecommunications operators to retain and/or provide data to the government (ss 158(6), 168, 170); and Bulk CD CoP [3.3] states that

---

115 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [78]–[79].

116 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [74].

117 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [81] (emphasis added).

118 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [29], [33].

a bulk acquisition warrant may relate to communications data retained by an operator for business purposes or under the provisions of Part 4 of the Act.

84. The other impugned provisions are also within the material scope of EU law. They too are indistinguishable for this purpose of the application of EU law from the powers considered in *Watson*. Further:

(1) All other impugned provisions (Part 5, Part 6 Chapter 1 and Part 6 Chapter 3), save those under Part 7:

(a) Allow the imposition of requirements on third parties, such as telecommunications operators, to give effect to warrants and impose particular duties on telecommunications operators to cooperate by retaining or obtaining content or communications data and providing this to state authorities;[119] and/or

(b) Depend in practice on the cooperation of CSPs, which will necessarily involve the processing of personal data by the cooperating CSP (for example, by transferring it to the government); and/or

(c) Govern the activities of providers of electronic communications services.

(1A) The conscription of telecommunications operators to enable all interception and hacking activities is further demonstrated by the Act's provisions on technical capability notices ("**TCN**"), regulations made to facilitate the exercise of those powers, and provision of public moneys to telecommunications operators in relation to their costs in complying with such notices:

(a) Under s 253(1) and (3), the Secretary of State may give a (proposed) telecommunications operator a "technical capability notice" (TCN) if this is considered necessary for securing that the operator has the capability to provide any assistance which the operator may be required to provide in relation (relevantly) to any warrant under Chapters 5 or 6, proportionate and is approved by a Judicial Commissioner.

[119] Sections 149(1) and (5) (bulk interception warrants — Pt 6 Ch 1), s 190(1) and (5) (bulk equipment interference warrants — Pt 6 Ch 3), ss 126, 128 (equipment interference warrants — Pt 5).

(b) A TCN may impose on the (proposed) telecommunications operator "*any applicable obligations specified in the notice*" (s 253(2)(a)) and requires the person to take all the steps specified in the notice for the purpose of complying with those obligations (s 253(2)(b)). A person to whom a TCN is given must comply with it: s 255(9)–(10).

(c) An "*applicable obligation*" means an obligation prescribed by regulations (s 253(3)). The Investigatory Powers (Technical Capability) Regulations 2018 (SI 2018/353) (the "**TCN Regulations**") prescribe obligations that may be imposed on telecommunications operators (reg 3(1)). Schedule 1 Part 1 prescribes applicable obligations (relevantly) for bulk interception warrants under Chapter 6 Part 1, Schedule 2 Part 1 prescribes applicable obligations (relevantly) for bulk acquisition warrants under Chapter 6 Part 2, and Schedule 3 prescribes applicable obligations for hacking and bulk hacking warrants under Part 5 and Chapter 6 Part 3: reg 3(2)–(4).[119a] Liberty relies upon the whole of the TCN Regulations. By way of illustration, the applicable obligations they prescribe include:

(i) In Part 1 of Schedule 1 (relating to bulk interception), obligations to:

(A) maintain the capability to carry out the interception of communications or secondary data and disclosed anything obtained under a warrant within one working day (meaning a period of 24 hours, not including time that is not a working day) (para 1);

(B) provide, modify, test, develop or maintain any apparatus, systems or other facilities or services necessary to provide and maintain that capability (para 2);

(C) provide and maintain the capability to ensure the interception, in their entirety, of all communications and the obtaining, in their

[119a] Regulation 4(3) prescribes that obligations in Part 1 of Schedule 1 and in Schedule 3 may not be imposed on a telecommunications operator who does not provide, nor intend to provide, a telecommunications service to more than 10,000 persons.

entirety, of all secondary data authorised or required by a warrant (para 3);

(D) provide and maintain the capability to ensure, where reasonably practicable, the transmission of communications and secondary data, as near to in real time as is reasonably practicable, to a hand-over point as agreed with the person to whom a warrant is addressed (para 4);

(E) provide and maintain the capability to ensure, where reasonably practicable, the transmission of communications and secondary data, as near to in real time as is reasonably practicable, to a hand-over point as agreed with the person to whom a warrant is addressed (para 6);

(F) provide and maintain the capability to disclose the content of communications or secondary data in an intelligible form where reasonably practicable, remove electronic protection applied by or on behalf of the telecommunications operator to the communications or data where reasonably practicable, or permit the person to whom a warrant is addressed to remove such electronic protection (para 8);

(G) provide and maintain the capability to simultaneously intercept (or obtain secondary data from) communications of 1 in 10,000 of the persons in the United Kingdom to whom the telecommunications operator provides that service (or such smaller number as specified in the notice) (para 9); and

(H) to put in place and maintain arrangements agreed with the Secretary of State to tell the Secretary of State of proposed changes to telecommunication services or systems to which the TCN relates or specified in the TCN and the development of new telecommunications services or systems (para 13);

(ii) In Part 1 of Schedule 2 (relating to bulk communications data), obligations to:

(A) provide and maintain the capability to obtain and disclose communications data "*without undue delay*" and within a period agreed between the telecommunications operator and the Secretary of State or specified in the TCN (para 1);

(B) provide, modify, test, develop or maintain any apparatus, systems or other facilities or services necessary to provide and maintain that capability (para 2);

(C) provide and maintain the capability to ensure the obtaining and disclosure, in their entirety, of all communications data to which an authorisation or warrant relates (para 4);

(D) ensure the transmission of the communications data to a hand-over point in accordance with levels of service specified in the notice or agreed between the telecommunications operator and the Secretary of State (para 5);

(E) provide and maintain the capability to disclose the communications data in an intelligible form where reasonably practicable, remove electronic protection applied by or on behalf of the telecommunications operator to the communications data where reasonably practicable, or permit the person authorised to obtain the communications data or to whom a warrant is addressed to remove such electronic protection (para 9);

(F) install and maintain any apparatus provided to the operator by or on behalf of the Secretary of State for the purpose of enabling the operator to obtain or disclose communications data (para 10);

(G) to put in place and maintain arrangements agreed with the Secretary of State to tell the Secretary of State of proposed changes to telecommunication services or systems to which the

TCN relates or specified in the TCN and the development of new telecommunications services or systems (para 13);

(iii) In Schedule 3 (relating to hacking and bulk hacking), obligations to:

(A) provide and maintain the capability for interference with equipment to be carried out for the purpose of obtaining any information at all (including communications or equipment data) with such period of service of a warrant as is specified in the TCN (para 1);

(B) provide and maintain the capability to ensure the obtaining of any information at all (including communications or equipment data) authorised by a warrant and to disclose anything obtained within such the period specified in the TCN (para 2);

(C) provide and maintain the capability to enable the transmission to the person to whom a warrant is addressed of any data of a type specified in the TCN that is required to secure equipment interference (para 3);

(D) provide, modify, test, develop or maintain any apparatus, systems or other facilities or services necessary to provide and maintain all of those capabilities (para 4);

(E) provide and maintain the capability to disclose any information in an intelligible form to standards specified in the TCN where reasonably practicable, remove electronic protection applied by or on behalf of the telecommunications operator to any information where reasonably practicable, or permit the person to whom a warrant is addressed to remove such electronic protection (para 6);

(F) provide and maintain the capability to disclose any information (including communications and equipment data) in such a way that the equipment data can be unambiguously correlated with

the communication or other item of information it was comprised in, included as part of, attached to or logically associated with (para 7);

(G) ensure that any hand-over interface complies with any appropriate industry standard, or other requirement, specified in the TCN (para 8); and

(H) to put in place and maintain arrangements agreed with the Secretary of State to tell the Secretary of State of proposed changes to telecommunication services or systems to which the TCN relates or specified in the TCN and the development of new telecommunications services or systems (para 11).

(d) Section 249(1) requires the Secretary of State to ensure that arrangements are in force for securing that telecommunications operators receive an "*appropriate contribution*" for "*relevant costs*". These are costs that telecommunications operators incur or are likely to incur in complying with the Act.

(i) By virtue of the foregoing provisions, this includes costs incurred or likely to be incurred in complying with TCNs.[119b] By s 249(8), the Secretary of State has power to make or arrange payments out of money provided by Parliament for this purpose. For example, the Bulk Interception CoP states, in relation to a TCN, that such payments may be made for "*the procurement or design of systems required to intercept communications,* [and] *their testing, implementation, continued operation*" and for "[c]*ertain overheads*", including staff employed "*specifically to manage compliance with the requirements under the Act*".[119c]

(ii) Section 249(1) applies also to costs incurred in giving effect to warrants. The Bulk Interception CoP, Bulk CD CoP and Bulk EI CoP

[119b] Bulk Interception CoP [8.50]–[8.57] recognises this.

[119c] Bulk Interception CoP [8.53].

make this clear and contain similar provision in relation to payment of costs incurred by telecommunications operators.[119d] The United Kingdom's notification to the EU of the TCN Regulations states: "*The cost recovery arrangements will also ensure that there is no additional impact on small firms which have obligations placed on them.*"[119e] Similarly, the United Kingdom's notification of the Act to the EU states:[119f]

> "The UK Government has committed to fully meet the costs of telecommunications operators complying with any new requirements to retain internet connection records. The costs met by Government will represent only the marginal costs resulting from the legal obligations placed on operators, not the normal costs of business, so no commercial benefit would be conferred upon operators as a result of this legislation."

Accordingly, it appears that the Secretary of State will pay to telecommunications operators the entirety of their costs of compliance with the Act.

(1B) Bulk Interception CoP [6.7] indicates that, in practice, "[a] *bulk interception warrant will usually be served on a telecommunications operator to provide assistance with giving effect to it*". Similarly, Bulk EI CoP [7.5] indicates that telecommunications and other persons may be conscripted to give effect to a warrant, stating that "[a]*ssistance sought will typically comprise (but may not be limited to) the provision of infrastructure by a relevant telecommunications operator, or details about the technical specification of relevant equipment*".

(2) Part 7 forms part of the storage/access regime for data obtained under other powers under the Act, except data obtained under a bulk acquisition warrant (see s 225),

---

[119d] Bulk Interception CoP [7.13]–[7.18]; Bulk CD CoP [8.1]–[8.7]; Bulk EI CoP [7.20]–[7.25].

[119e] Notification No 2017/332/UK, 13 July 2017 (available at <http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2017&num=332>). Remarkably, notwithstanding the concessions made on 7 July 2017 in relation to Part 4 (see paragraph 29K above), this notification states without qualification: "*The powers provided for in the Investigatory Powers Act 2016 are consistent with Directive 2002/58/EC on the processing of data and protection of privacy in electronic communications under the derogations at Article 15(1).*"

[119f] Notification No 2016/384/UK, 25 July 2016 (available at <http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2016&num=384>).

so falls within the material scope of EU law (which continues to apply to data obtained by the state by measures within the material scope of EU law) on the same basis. In addition, ~~they~~ Part 7 falls within the material scope of EU law because intelligence services will obtain bulk personal datasets (which must be electronic) only, generally and/or in some instances~~,~~ from non-government third parties, such as telecommunications operators, who in providing them will process personal data and/or provide the personal data to government via telecommunications systems.

84A. As set out in paragraphs 81–84 above, the impugned provisions either (i) operate by requiring CSPs (and other third parties) to provide content, secondary data, communications data and/or other information to national authorities (ie the state) or (ii) expressly permit requirements to be imposed upon CSPs and any other third party to do so or to assist the state in obtaining such data (which will, or may, entail the processing of personal data). They are accordingly within the material scope of EU law at least to that extent. The impugned provisions do not distinguish, in relation to the obtaining, retention, use and/or other processing of data by the state, between data obtained by measures within the material scope of EU law (for example, any data obtained from or via a public telecommunications network) and otherwise (for example, by activities carried on exclusively by the state without any involvement of third parties, which may in principle fall outside the material scope of EU law: see *PI* [48]). Because the impugned provisions do not so distinguish, and because the EU law requirements set out below are quality of law requirements (they require a legislative regime to make certain provision), it is necessary as a practical matter for the impugned provisions to satisfy the EU law set out below in all their applications, so that, insofar as they are applied within the scope of EU law, they comply with it.

(b) Constraints imposed by EU law

85. The impugned provisions interfere with the rights protected by Articles 7 ("Respect for private and family life"), 8 ("Protection of personal data") and Article 11 ("Freedom of expression and information") of the CFR, in the last case due to their inevitable impact on the use made of electronic communications.[120]

[120] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [101].

86. The impugned provisions must therefore comply with Article 52(1) of the CFR. Further, the powers under challenge derogate from rights protected by Articles 5, 6, 8(1),(2),(3) and (4) and 9 of Directive 2002/58 ("the e-Privacy Directive"), so are subject to the constraints set out in Article 15(1) of that Directive (set out in paragraph 75 above).

87. Together Article 52(1) of the CFR, Article 15(1) of the Directive and *Watson* (and subsequent decisions such as *PI* and *La Quadrature*) require that measures that interfere with the rights they confer:

(1) Are "*provided for by law*" (Article 52(1) of the CFR) and are "*legislative measures*" (Article 15(1) of Directive 2002/58) — both are quality of law requirements, although the latter is a higher standard requiring legislation;

(2) Pursue an objective in the general interest (Article 51(1) of the CFR) that is included in Article 15(1) of the Directive and is sufficiently important;

(3) Respect the essence of the rights with which they interfere (Article 51(1) of the CFR); and

(4) Are strictly necessary and proportionate, in particular complying with the mandatory requirements set down in *Watson* and maintained (with some qualifications in relation to "national security", defined in a narrow sense as explained below) in *PI* and *La Quadrature*.

~~87A. In addition, Article 18 TFEU and Article 21 CFR prohibit discrimination based on nationality, national origin and/or residence. Any such discrimination must be justified.~~

87B. The requirements summarised in paragraph 87 above and explained below in greater detail constitute general principles of EU law. That includes in particular the right under Article 5 of e-Privacy Directive to confidentiality and privacy of communications, and the equivalent protection under CFR Articles 7, 8 and 11.

Quality of law

88. *Watson* establishes that the requirement in Article 15(1) of Directive 2002/58 for "*legislative measures*" means that any measures that interfere with the rights set out

above must be "*legally binding under domestic law*".[121] In so holding, the CJEU accepted the Advocate General's conclusions that Article 15(1) permits only measures that are "*binding on the national authorities upon which the power to access the retained data is conferred*",[122] that is, "*legislative or regulatory measures*", and not "*codes of practice or internal guidelines having no binding effect*".[123] *La Quadrature* at [132] reinforces that the provisions required to satisfy the *Watson* requirements must be "*legislation*" that is "*legally binding*".

89. Accordingly, should the Defendants seek to rely on any ~~(as yet unpublished)~~ codes of practice or other guidelines, this will not assist them under EU law. EU law does not permit regard to anything that is not legislation or regulation in English domestic terms (that is, anything that does not have the force of law) in assessing the compatibility of the impugned provisions.[124]

90. In any case, because the protection under CFR Articles 7 and 11 is at least equivalent to that under ECHR Articles 8 and 10 respectively (see paragraph 105 below), at a minimum the requirements under the ECHR explained above for accessibility and foreseeability apply also under EU law. Accordingly, the Defendants may not rely on any non-public document to justify the impugned provisions under EU law.

Pursuit of an objective in the general interest

91. The CJEU held in *Watson*, *PI* at [74]–[75] and *La Quadrature* at [134]–[139], [141], [163]–[165] that only the objectives of fighting serious crime and protection of "national security" as defined by the CJEU, that is, limited to the most serious such threats (see paragraph 96B below), could justify any non-individualised obligation to retain or provide access to data under Article 15(1) of Directive 2002/58 (although, as explained below, a power that could be used to impose a general and indiscriminate data retention

---

121 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [117].

122 Opinion of Advocate-General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Watson* ECLI:EU:C:2016:572 [150].

123 Opinion of Advocate-General in *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:572 [150]–[151].

124 Codes of practice under Schedule 7 of the Act are therefore irrelevant to the question of compatibility with EU law. Schedule 7 does not require that a code of practice be followed or otherwise give it the force of law (see Sch 7 paragraph 6). The Act expressly provides that a failure to follow a code of practice does not carry civil or criminal liability.

obligation, as in issue in *Watson* under DRIPA, is in no circumstances compatible with EU law, save where its purpose is protecting national security in the limited sense just mentioned). This applies both to the retention of communications data by CSPs[125] and access to such data by state authorities.[126]

92. ~~Alternatively, Watson establishes that only serious threats to the interests protected by secret surveillance legislation is capable of justifying a measure which provides for the retention of communications data (or more invasive information).~~[127]

Respect for the essence of the rights and freedoms

93. Article 52(1) of the CFR requires that limitations on rights "*respect the essence of th*[e] *rights and freedoms*". In the context of surveillance regimes, in *Schrems* the CJEU said:[128]

> "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter".

94. *Watson* confirms that legislation that permits the general and indiscriminate "*retention of the content of a communication*" (as well as permitting access thereto) adversely affects the essence of the rights under Articles 7 and 8 of the CFR.[129] *PI* (especially at [80]–[81]) and *La Quadrature* proceed on that basis.

Prohibition on provisions requiring or permitting general retention

95. *Watson*, *PI* (see especially at [80]–[82]) and *La Quadrature* establishes that generalised and indiscriminate retention of communications data (or, it follows, content or secondary data) by CSPs, even for the purpose of fighting serious crime and for any other purpose (other than preventing the most serious threats to national security: see paragraph 96B below), can never be strictly necessary. Whereas the Advocate General in *Watson* had

---

125 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [102].

126 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [115].

127 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [102].

128 Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [94] (citations omitted).

129 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [101].

suggested that the objective of fighting serious crime could justify a general data retention obligation (subject to adequate safeguards), the CJEU in *Watson* held that:[130]

> "… such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight."

The CJEU in both *PI* at [74]–[75] and *La Quadrature* [134]–[139], [141]–[142], [163]–[165] affirmed this.

96. The Court in *Watson* went on to make clear that Member States may only adopt legislation which permits, "*as a preventative measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*"[131]

96A. *La Quadrature* at [140]–[147] and [160]–[167] further establishes that, in addition to the purpose of fighting serious crime, only the purpose of preventing serious threats to public security (and protecting national security: see paragraph 96B below) is of its nature capable of justifying measures that effect such a serious interference with the rights under CFR Articles 7 and 8 (and, the Claimants aver, Article 11) as is constituted by requiring CSPs to effect the preventive retention of traffic and location data. National law that permits preventative retention by CSPs for other purposes is without more incompatible with EU law. Further, the purpose of preventing a serious threat to public security, like that of preventing and detecting serious crime, is incapable of justifying a regime of general and indiscriminate retention by CSPs (but may in principle justify a targeted regime): *La Quadrature* at [141]–[142].

96B. The Claimant accepts that *PI* at [74] and [80]–[82] and *La Quadrature* at [137] establish that the purpose of protecting "national security" (in the limited manner there defined), and no other purpose, may in principle justify a regime of preventative generalised

---

130 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [103]; see also [107], [112].

131 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [108] (emphasis added).

retention of traffic and location data by CSPs, if that regime has sufficient safeguards in particular as to access by the state (as to which see below). For this purpose, protecting national security is limited in scope to "*the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself*": *PI* at [74]; *La Quadrature* at [135]. Such risks are to be "*distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise*": *PI* [75]; *La Quadrature* [136]. Further, "*national security*" as defined by the CJEU for these purposes refers only to "*a serious threat to national security that is shown to be genuine and present or foreseeable*": *La Quadrature* [168] (first indent). Outside of the narrow definition of protecting national security laid down in those cases, a regime of preventative generalised retention by CSPs of traffic and location data is, without more, incompatible with EU law.

Safeguards/Mandatory requirements

97. Additionally, *Digital Rights Ireland*, *Schrems* and *Watson* as well as *PI* at [68] and *La Quadrature* at [132] establish that legislation that interferes with rights under Articles 7 and 8 of the CFR must lay down:[132]

> "clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data …"

98. The need for safeguards is "*all the greater*" where there is automatic processing of data or "*a significant risk of unlawful access*".[133] Any interference must go no further than "*strictly necessary*".[134] *Digital Rights Ireland* held that the interference with the rights

---

[132] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [54]; repeated in Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [91] (emphasis added) and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [109].

[133] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [55]; Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [91].

[134] Case C-362/14 *Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [92]; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [52].

was serious and the rights in issue (under Articles 7 and 8 of the CFR) important, so the legislature's "*discretion is reduced*".[135]

99. The substantive and procedural requirements (explained immediately below) that *Watson* and *La Quadrature* (at [160]–[167]) confirms must be satisfied in relation to a data retention obligation or state power to access electronic data under EU law are referred to as the "***Watson* requirements**". These requirements apply save where the purpose of a national measure is preventing the most serious threats to national security, as to which the requirements set out in paragraph 102A below apply.

100. *Watson* clarified that national legislation governing the scope and application of a measure permitting retention of or access to electronic data must:

(1) Ensure that the continued retention of or access to data meets objective criteria that establish a connection between the data to be retained and the objective pursued and, further, that "*such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected*";[136] and

(2) Set limits to retention or access based on "*objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security*".[137]

101. The CJEU also clarified that legislation will exceed the limits of what is strictly necessary where:

(1) It does not require there to be any relationship between the data which must be retained or to which access must be provided and a threat to public security. This is the case where retention "*is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii)*

---

135 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [48].

136 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [110]. The judgment at [117] makes clear that the same requirements apply to retention and state access.

137 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [111].

persons who could, for other reasons, contribute, through their data being retained, to fighting crime".[138] *Digital Rights Ireland* states that a reference only "*in a general manner to serious crime*" is not sufficiently specific;[139]

(2) The retention period is not "*based on objective criteria such that it may be ensured that it is limited to what is strictly necessary*" so that where "*the retained data may be distinguished on the basis of their usefulness … the retention period* [must be] *adjusted on the basis of that criterion*".[140]

102. *Watson* establishes (and *La Quadrature* at [165] confirms) that any national legislation that permits the retention of communications data (and, it therefore follows, content and/or secondary data) must satisfy the following requirements, so as to be strictly necessary:

(1) **Purpose of access/use:** National legislation must lay down clear and precise rules indicating when CSPs must give national authorities access to data and "*as a general rule*" may permit access only to the data of individuals suspected of planning, committing or having committed or otherwise been implicated in a serious crime; however, vital national security, defence or public security interests may permit wider access outside of these categories "*in a specific case*".[141]

(2) **Process of access by authorities:**

~~(a) The access process must begin "following a reasoned request by [the] authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime", except in cases of validly established urgency.[142]~~

(b) National authorities' access to data "*should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either*

---

138 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [106].

139 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [60].

140 Opinion of Advocate-General in *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:572 [242], citing Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [63]–[64].

141 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [117], [119].

~~142 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [120].~~

by a court or by an independent administrative body", to ensure that the conditions of strict necessity are met.[143] To that end, the access process must begin "*following a reasoned request by* [the] *authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime*", except in cases of validly established urgency.[143a]

(c) Also to that end and ~~C~~consistently with *Watson*, *PI* and *La Quadrature*, the Advocate General in *Watson* ~~had~~ made clear that urgency procedures must apply only "*in specific situations of extreme urgency*" where "*an application for access to an independent body is incompatible*" with that urgency.[144]

(3) **Notification after retention/access:** National legislation must require notification of any person affected by electronic surveillance as soon as that notification is no longer liable to jeopardise the investigations being undertaken.[145] This is necessary to enable those affected to seek legal redress under Article 15(2) of the Directive and therefore required also by the right to a legal remedy in EU law.[146]

(4) **Retention:** National law must require:

(a) Data to be retained within the EU;[147]

(b) Providers of electronic communications services to guarantee a particularly high level of protection;[148] and

(c) "[T]*he irreversible destruction of the data at the end of the data retention period*",[149] which, as the Advocate General pointed out, applies both to service providers who retain and national authorities who access the data.[150]

---

143 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [120].

143a Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [120].

144 Opinion of Advocate-General in *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:572 [237].

145 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [121].

146 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [121].

147 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [122].

148 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [122].

149 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [122].

150 Opinion of Advocate-General in *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:572 [243]; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 64.

(5) **Independent review of compliance:** National law must ensure review, by an independent authority, of compliance with the level of data protection required by EU law.[151]

102A. Insofar as any national measure provides for preventative general and indiscriminate retention of traffic and location data by CSPs and for (appropriately limited) access to it by the state for the purpose of preventing the most serious threats to national security (the only purpose for which this is permitted), *PI* [65], [67]–[68], [74]–[82] and *La Quadrature* [134]–[139] indicate that any such measure:

(1) Must, as a bare minimum, contain sufficient safeguards to comply with the requirements of the ECHR under Articles 8 and 10 (see especially *PI* [67]–[68], [76], [78]);[151a]

(2) Cannot permit general and indiscriminate retention or access by the state, including general and indiscriminate transmission to the state of retained data (see *PI* at [80]–[82]);

(3) In addition, must (see especially *La Quadrature* [138]–[139]):

(a) expressly be limited to the purpose of preventing a "serious threat to national security that is shown to be genuine and present or foreseeable", that is, to verifiable threats to national security in the narrow sense explained above;

---

[151] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [123].

[151a] The CJEU requires that, for a generalised regime, "the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned" (*PI* at [65]), that derogations from the principle of confidentiality of communications must apply only insofar as is strictly necessary (*PI* at [67]), and that "the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse", legislation must "be legally binding under domestic law", and must "indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary" (*PI* at 68). The CJEU lays down requirements as to access that "legislation cannot confine itself to requiring that authorities' access to the data be consistent with the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use" (*PI* at [77]) and further that "national legislation governing access to traffic data and location data must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue" (*PI* at [78]). Without conceding that EU law does not impose any more stringent or particular requirements (particularly where content and/or secondary data is retained and/or accessed), Liberty assumes for present purposes that these requirements are substantively equivalent to those that apply under the ECHR for secret surveillance regimes.

(b) require instructions to third parties to retain data to be "limited in time to what is strictly necessary" and not to exceed a foreseeable period of time, albeit with the possibility of renewal;

(c) provide that retention of data is "subject to limitations" and "circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons concerned against the risk of abuse", so that retention is not "systematic in nature";

(d) require "effective review" of each decision to instruct third parties to retain traffic and location data (by a court or administrative body whose decision is binding), which considers whether (i) a sufficiently serious threat to national security exists and (ii) that the required conditions and safeguards are laid down;

(e) in accordance with general principles of EU law, provide an effective remedy for all EU nationals whose data might be unlawfully retained or accessed.

102B. Further, *La Quadrature* [176]–[182] establish that any regime that provides for or entails general and indiscriminate processing by CSPs of retained data (which is in principle only permissible for the purpose of protecting national security, in the narrow sense just explained) must comply with the requirements in paragraph 102A below and in addition must require that:

(1) Any model or criteria used for automatic processing must be:

(a) Specific and reliable, such that it can in practice identify persons who might reasonably be suspected of participating in activities that pose the most serious threats to national security;

(b) Non-discriminatory, and in particular, not be based on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person's health or sex life in isolation;

(c) Regularly re-examined, to ensure that the model or criteria remain reliable and up-to-date; and

(2) Any positive result from such analysis is subject to individual re-examination by non-automated means before a measure adversely affecting an individual is adopted.

It is unclear whether any of the impugned provisions permit the imposition of requirements on CSPs to carry out extensive automated processing on behalf of the state. If and to the extent they do so (and, further, if and to the extent that the state itself may carry out such processing under those provisions), the impugned provisions do not contain requirements equivalent to those set out immediately above, and are to that extent incompatible with EU law.

102C. *Watson*, *La Quadrature* and *PI* all consider regimes that provide for the retention of and/or state access to communications data, and not more intrusive forms of personal data, such as secondary data and content (as defined under the Act). In general, the more intrusive a measure, the greater must be its justification and, in the context of quality of law requirements for secret surveillance regimes, the more stringent are the safeguards required. Liberty therefore reserves the right to contend that:

(2) Insofar as national measures for the purpose of preventing the most serious threats to national security permit the retention and/or use and/or other processing of content and/or secondary data, the requirements set out in paragraph 102 above (and/or greater requirements for safeguards) apply; and/or

(2) Insofar as national measures for the purposes of fighting serious crime and/or preventing a serious threat to public security permit the retention and/or use and/or other processing of content and/or secondary data, greater requirements than those set out in paragraph 102 apply.

103. As set out below in relation to each power, the impugned powers do not comply in various respects with the *Watson* requirements, insofar as those requirements apply. For example, none of the challenged provisions:

~~(1) Limits access to data obtained/retained under the powers to the data of those suspected of serious crimes (or, alternatively, to serious threats to the interests protected);~~

(2) Requires a reasoned request and prior judicial or other independent authorisation each time data is accessed (save for Part 4, as amended, in light of this claim having been brought and the Defendants' eventual concession that it was incompatible with EU law because it did not provide for prior independent authorisation of access: see paragraph 29K above); or

(3) Requires after-the-event notification once this is possible in all cases (notwithstanding limited provision for notification by the Investigatory Powers Commissioner of "*serious errors*" under s 231).

104. Liberty submits that, given the current dialogue that exists between the ECtHR and the CJEU on issues of secret surveillance regimes,[152] the *Watson* requirements reflect also the requirements under ECHR Articles 8 and 10.

~~Discrimination~~

~~104A. The first paragraph of Article 18 TFEU provides:~~

> ~~"Within the scope of application of the Treaties, and without prejudice to any special provisions contained therein, any discrimination on grounds of nationality shall be prohibited."~~

~~104B. Article 21 CFR provides:~~

> ~~"1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.~~
>
> ~~2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited."~~

~~104C. EU law therefore prevents discrimination as follows:~~

---

152 *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [23], [70], citing Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [26], [27], [52], [62]; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [119]–[120], citing *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [260] and *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [77], [80].

~~(1) Article 18 TFEU and Article 21(2) CFR prohibit discrimination on grounds of nationality within the scope of application of the Treaties; and~~

~~(2) Article 21(1) CFR prohibits discrimination based on "any ground" (within the scope of EU law).~~

~~104D. Any such discrimination must be justified. Discrimination based on nationality may be justified "only if it is based on objective considerations independent of the nationality of the persons concerned and is proportionate to the objective being legitimately pursued".[120a] Discrimination on "any ground" must be justified under Article 52(1) CFR. The Defendants bear the burden of establishing that any discrimination is justified.~~

(c) CFR Articles 7 and 11 and journalistic sources / lawyer–client communications

105. CFR Articles 7 and 11 correspond to ECHR Articles 8 and 10 respectively,[153] so "*the meaning and scope of those rights shall be the same as those laid down by the* [ECHR]".[154] Accordingly, the requirements in relation to journalistic sources and lawyer–client communications under ECHR Articles 8 and 10 (see paragraphs 67 and 71 above) are required also by Article 11 CFR. The Divisional Court in *Davis & Watson* held correctly that "*communications with ... journalists ... require special consideration*".[155]

106. Further, as explained in paragraphs 88–89 above, for EU law, limits to the interference with this right must derogation must be imposed by provisions with the force of law rather than a code of practice.

~~*(d) Prohibitions on discrimination under Article 18 TFEU and Article 21 CFR*~~

~~106A. Liberty repeats paragraphs 71F–71K above mutatis mutandis in relation to EU nationals other that UK nationals and the safeguards in Chapter 6 Part 1 and Chapter 6 Part 3 that turn on whether a person is known to be physically present in the United Kingdom when~~

~~[120a] Case C-524/06 Huber v Germany ECLI:EU:C:2008:724 [75].~~

153 Explanations Relating to the Charter of Fundamental Rights [2007] OJ C 303/02, 21.

154 CFR Article 52(3).

155 *R (Davis & Watson) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) [98] (Bean LJ. See also Opinion of Advocate-General in *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:572 [235].

communications or other information obtained are "selected for examination". In summary, unlawful discrimination under EU law arises because:

(1) As set out above, the impugned provisions fall within the material scope of EU law;[155a]

(2) It is the case that:

(a) A British citizen is substantially more likely to be present in the British Islands than a non-British EU citizen;

(b) An EU citizen of British national origin is substantially more likely to be present in the British Islands than an EU citizen who is not of British national origin; and

(c) An EU citizen who is resident in the United Kingdom is substantially more likely to be present in the British Islands than an EU citizen who is not resident in the United Kingdom.

(3) The application of a safeguard where communications or information are "selected for examination" only where a person is known to be present in the British Islands discriminates as follows:

(d) A British citizen is substantially more likely to have that safeguard applied to the "selection for examination" of their communications or information than a non-British EU citizen;

(e) An EU citizen of British national origin is substantially more likely to have that safeguard applied to the "selection for examination" of their communications or information than an EU citizen not of British national origin; and

(f) An EU citizen who is resident in the United Kingdom is substantially more likely to have that safeguard applied to the "selection for examination" of their communications or information than an EU citizen who is not resident in the British Islands.

[155a] As to this requirement, see, eg, Case C-524/06 Huber v Germany ECLI:EU:C:2008:724 [70].

~~(4) The discrimination identified in paragraph 106A(3)(a) above is prohibited by Article 18 TFEU and Article 21(2) CFR as indirect discrimination on grounds of nationality, and that identified in paragraphs 106A(3)(b)–(c) above is prohibited by Article 21(1) CFR as indirect discrimination based on "any ground". Accordingly, it is for the Defendants to justify that discrimination. Should the Defendants seek to advance any justification, Liberty may seek to respond either by submissions or evidence as appropriate, including before permission is given. For the reasons in paragraphs 71L–71N above, any justifications the Defendants may advance are unlikely to withstand scrutiny.~~

D GROUNDS OF CHALLENGE: BULK INTERCEPTION (PART 6 CHAPTER 1)

107. A brief overview of Part 6 Chapter 1 is at paragraph 18(1) above. It permits the issue of bulk interception warrants, which, in broad summary:

(1) May authorise or require any one or more of: (i) the interception of communications in the course of their transmission (that is, capture of content); (ii) the obtaining of "secondary data" from such communications; (iii) the "selection for examination" of intercepted content or secondary data; and/or (iv) the disclosure of anything obtained under the warrant to its addressee (s 136(4));

(2) Must have as their "main" purpose either or both of the (i) interception of overseas-related communications or (ii) obtaining secondary data from them (s 136(2)), which are communications sent or received by individuals outside the British Islands (s 136(3));

(3) May be issued by the Secretary of State where considered necessary and proportionate in the interests of national security (or national security and other interests)[156] (s 138(1)) to the head of an intelligence service (s 142(2)); and

(4) Where they authorise "*selection for examination*" of intercepted content, must specify the "operational purposes" for which selection for examination of intercepted content is or may be necessary (ss 138(1)(d), 142(3)–(10)) — these are

[156] Preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom insofar as those interests are relevant to the interests of national security (s 138(2)).

purposes maintained in a list by the heads of the intelligence services, which must be specified in a greater level of detail than "*the interests of national security*", for which selection for examination may be necessary.

(1) Incompatibility with ECHR

(a) Absence of individual targeting and reasonable suspicion

108. The power to issue bulk interception warrants is incompatible with Articles 8 and 10 ECHR because these warrants are not:

(1) limited by reference to an individual/set of premises ~~(or an individual operation or investigation)~~; and/or

(2) permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

108A. Bulk Interception CoP [6.4] and [6.8] make clear that the Defendants consider (correctly) that the power to issue bulk interception warrants is not limited in those ways. At [6.4] it states that bulk interception may be used for example "*to identify patterns of activity that might indicate a threat to the United Kingdom*" and at [6.8] it indicates that bulk interception is "*a strategic intelligence gathering capability*" and contrasts this to targeted interception "*that is used once a particular subject for interception has been identified*".

(b) Consideration of critical factors

109. Further or alternatively, the power to issue bulk interception warrants is incompatible with Articles 8 and 10 ECHR because it lacks sufficient safeguards, detail and clarity as to each of the critical features (and, further, the critical features taken together) in the following respects:

110. **Scope of application:** The scope of and level of discretion conferred by the bulk interception warrant provisions is wide. They grant the "*almost unlimited degree of*

discretion" and expressly enable the "*strategic, large-scale interception*" which concerned the ECtHR in *Zakharov* and *Szabó*:[157]

(1) As stated, bulk interception warrants are not limited by reference to an individual or~~,~~ set of premises~~, a particular operation or a particular investigation~~, nor do they require any factual suspicion of a particular person (even when examining communications that have been intercepted).[158]

(2) The requirement that a bulk interception warrant have a "*main purpose*" of interception of "*overseas-related communications*" (or obtaining secondary data from them) (s 136(2)) permits other undefined subsidiary purposes, which include intercepting intra-UK communications. Further, it is in practice impossible to know whether a communication is "*overseas-related*" as defined in s 136(3) until it is captured and the physical location of its sender/recipient is known, so this apparent limitation on "main purpose" is unlikely in practice to reduce the extent of any capture or otherwise provide any real limitation on the power to issue a warrant. In addition, the definition of "*overseas-related communications*" appears to encompass communications sent to or received by individuals who are outside the British Islands at any point of the transmission of the communication (which will occur with virtually all internet-based communications), even where the ultimate sender and recipient are in the British Islands.[158a]

(3) Bulk interception warrants permit or require interception (s 136(4)), which creates further discretion for the executive.

---

157 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [248].

158 This includes where a targeted examination warrant is necessary under s 152 (see ss 17(2) and 20(2), which do not limit a targeted examination warrant to a particular individual or~~,~~ set of premises ~~or operation/investigation~~ or require any reasonable suspicion).

158a For these reasons, the purported requirement in Bulk Interception CoP [6.10] for an intercepting authority to use its knowledge of the way in which international communications are routed and "*regular surveys of communications links*" to identify communications links that are most likely to contain overseas-related communications, and to conduct interception "*in ways that limit the interception of communications or rescondary data that are not overseas-related to the minimum level compatible with the objective of intercepting the required overseas-related communications*", do nothing to restrict the scope of communications that may be intercepted. In any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(4) There is no closed list of offences for which the power may be exercised (the only limit being "*the interests of national security*"), nor is the power directed exclusively to overseas communications. The power is therefore wider than that considered in *Weber and Saravia v Germany*.[159]

(5) The requirements that a warrant be necessary and proportionate in the interests of national security (with or without further grounds) do little to identify or circumscribe the circumstances in which the content of communications may be intercepted under a warrant. It seems that a warrant may, for example, permit the interception of all communications transmitted on a particular route (such as an undersea cable). Bulk Interception CoP [6.6]–[6.8] confirms that this understanding accords with the Defendants' own view of the scope of the power. It explains that bulk interception may in principle entail the interception (retention) of "*all communications transmitted on a particular route or cable, or carried by a particular telecommunications operator*" and that "*interception will result in the collection of large volumes of communications and/or data*", all of which is then "*filtered*" and some of which may be discarded.

(6) The operational purposes do not limit interception (retention) at all, as they apply only at the point of "selection for examination" (see ss 150(1)(b), 152(1)(a) and 152(2)). Operational purposes may be included in a warrant where "selection for examination" for the operational purpose is considered necessary for **any** of national security, preventing and detecting serious crime or economic wellbeing insofar as it relates to national security, not necessarily just for national security: s 138(1)(d)(ii).[159a] ~~They~~The operational purposes do little to identify or circumscribe the circumstances in which the content of communications may be examined. As a matter of construction, the provisions limiting selection for examination (s 152) do not prevent all examination or **disclosure** of intercepted material, rather than selection for examination (and the latter is not necessary for

[159] *Weber and Saravia v Germany* (App No 54934/00, 29 June 2006, Third Section) [27], [29], [115] (broad range of interception subjects but surveillance limited to surveillance to "*certain serious criminal acts*").

[159a] See Bulk Interception CoP [6.23].

the former to occur).[160] In any event, the operational purposes are only purposes for which examination may be necessary, are not required to be published, must under s 142(7) be specified "*in a greater level of detail*" than the purposes in s 138(1)(b) or (2) (but this is an undemanding standard),[160a] and it appears to be the government's intention that a bulk interception warrant (and, indeed, all bulk warrants) will generally specify the full range of operational purposes (as s 142(5) expressly permits). As the Solicitor General said during committee consideration of the Bill: "*In the majority of cases, it will … be necessary for bulk interception warrants to specify the full range of operational purposes in use at a particular time.*"[161] The Bulk Interception CoP confirms this.[161a] These purposes will together represent all purposes for which communications are ~~intercepted~~selected for examination at the time when the warrant is issued (see s 142(4) and Bulk

---

160 Under s 136(4), a bulk interception warrant could be issued that authorised only interception (s 136(4)(a)) and "*disclosure, in any manner described in the warrant, of anything obtained under the warrant*" (s 136(4)(d)) to the addressee, without authorising "*selection for examination*" (s 136(4)(c)). Nothing prevents the addressee, to whom the material ~~is~~ has been disclosed and is therefore available, from "*examin*[ing]" it (that is, reading, looking at or listening to it: s 263(7)). Section 152(1) is directed only to "*selection … for examination*". Section 152(2) states that selection for examination is carried out for the specified purposes "*if the intercepted content … is selected for examination only so far as is necessary for the operational purposes specified in the warrant*". Bulk Interception CoP [6.72] accepts implicitly that examination of material may occur without "selection for examination" in that it states: "*In general, automated systems should, where technically possible, be used to effect the selection for examination. A limited number of officials may also be permitted to access the system during the processes of filtering, processing and selection for examination, for example to check system health. Such access must itself be necessary on the grounds specified in sections 138(1)(b) and 138(2) and where such access involves selection for examination of content or secondary data it must be necessary for an operational purpose specific on the warrant.*"

160a The purported additional requirements in Bulk Interception CoP [6.63] that operational purposes must "*describe a clear requirement*" and "*contain sufficient detail to satisfy the Secretary of State that intercepted content or secondary data may only be selected for examination for specific reasons*" add nothing because: they are vague and subjective (and gloss s 142(7)); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

161 *Parliamentary Debates*, House of Commons, 21 April 2016, col 461 (Solicitor General Robert Buckland).

161a Bulk Interception CoP [6.67]–[6.68]:

"*In the majority of cases, it will be necessary for bulk interception warrants to specify the full range of operational purposes in relation to the selection for examination of intercepted content. This reflects the fact that bulk interception is a strategic capability and overseas-related communications relevant to multiple operational purposes will necessarily be transmitted and intercepted together under the authority of a bulk interception warrant.*

Other than in exceptional circumstances, it will always be necessary for every warrant application to require the full range of operational purposes to be specified in relation to the selection for examination of secondary data obtained under bulk interception warrants."

See also Bulk Interception CoP [6.14]: "*It is highly likely that a bulk interception warrant will specify the full range of operational purposes, as set out at section 142(5) …*"

Interception CoP [6.61]), so the requirement for operational purposes provides no real limitation beyond examination being necessary "*in the interests of national security*" (with or without other interests). (Further, if the operational purposes are not published, neither their existence nor their content may be taken into account in assessing the critical features: see paragraphs 45–46B above.)

Accordingly, the power is wider than that considered in *Kennedy v United Kingdom*[162] under RIPA s 8(1), which was in particular limited to warrants that applied to one person or a single set of premises, required the warrant to specify the factors by which intercepted material was to be examined, and did not permit "[i]*ndiscriminate capturing of vast amounts of communications*".[162a] ~~and~~It is analogous in its scope to that held incompatible with the ECHR in *Liberty v United Kingdom*.[163]

111. **Duration:** The duration of bulk interception warrants is six months, although they are subject to renewal (ss 143–4). A warrant must be cancelled where the Secretary of State or a senior official considers it no longer necessary or proportionate (s 148(2)). However, there is no statutory duty upon either the Secretary of State or a senior official to keep bulk interception warrants under review.[163a]

112. **Authorisation procedure:** The Secretary of State decides to issue a warrant and a Judicial Commissioner, who is independent of the executive, must approve that decision (ss 138(1), 140(1)). The Secretary of State considers the necessity and proportionality of the warrant, and the Judicial Commissioner reviews those conclusions. Nonetheless, the authorisation procedure will not ensure that surveillance is not ordered haphazardly, irregularly or without due and proper consideration because:

---

162 *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [159]–[160].

162a *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [40], [160].

163 *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [64]–[65].

163a The purported requirement upon intercepting authorities (not the Secretary of State) to keep warrants under review in Bulk Interception CoP [6.56] does not contribute to the certainty of the duration of a warrant because: it does not state who (which person) must do this, with what regularity, by what means or on the basis of what materials; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(1) Judicial Commissioners apply only a judicial review standard (s 140(2)), in circumstances where (i) the Secretary of State need not provide reasons for her decision and (ii) there is no opposition presented to the decision;[163b]

(2) The addressee of a warrant may require another person, including a telecommunications operator, to assist in giving effect to the warrant (s 149(1)). However, to do so, the addressee may serve only a schedule or a warrant without any schedules (s 149(2), (6)). As there is no statutory requirement to include anything in a schedule to a warrant, telecommunications operators (and anyone else on whom the warrant is served) are unable to check that a warrant is duly authorised or properly implemented;[164]

(3A) An operational purpose may be added to a warrant and, thereafter, material obtained previously may be selected for examination for this new operational purpose (s 145(2)(a)).[164a] Accordingly, a modification may allow intercepted material to be selected for examination for a purpose other than that for which it could have been selected for examination when obtained;

[163b] Further, the purported requirement in Bulk Interception CoP [6.19] that there is a review within the agency prior to an application being made does not increase the certainty of the authorisation procedure because: there is no requirement for the reviewer to be independent from the person or team seeking the authorisation; the reviewer is not empowered to prevent an application if they consider that an application is not necessary or proportionate or "selection for examination" would not be necessary for an operational purpose; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements for applications in Bulk Interception CoP [6.20] do not increase the certainty of the authorisation procedure because: they do not state that an application may not be made if it does not include (a satisfactory) explanation of any of the matters referred to (and do not make any other provision for this circumstance); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The purported requirement that a Judicial Commissioner has access to the same application as the Secretary of State in Bulk Interception CoP [6.28] also does not increase the certainty of the authorisation procedure because: there is no provision that a Judicial Commissioner may not approve a warrant if this is not the case; and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[164] Cf *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [269]: "*the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception*". Bulk Interception CoP [6.37] and [7.10] confirm that telecommunications operators will not be given entire warrants, in that they state that it is "*unlikely*" that telecommunications operators will receive a copy of the operational purposes specified in the warrant and that part only of a warrant may be given to a telecommunications operator. This makes it hard or impossible for a telecommunications operator to exercise supervision over whether interception and disclosure is in accordance with a warrant.

[164a] As stated in Bulk Interception CoP [6.47].

(3) A modification adding or varying an operational purpose may be made urgently and has effect for three working days without Judicial Commissioner approval (s 145(2), (3), (5)), there is no review of the decision to make the modification urgently (see s 147) and non-approval of the modification does not affect the lawfulness of conduct carried out under it (s 147(5));.

(4) Schedule 8 permits, but does not require, combinations of warrants, for which the most onerous authorisation procedure must be followed. However, because there is no requirement to combine warrants that affect the same persons, communications or information, where warrants are issued separately the authorisation procedure does not ensure that the totality of interference from related warrants is necessary and proportionate.

113. **Procedure for use/examination/storage/precautions when communicating:** Sections 150 and 152 require "arrangements" that create some safeguards for use, examination, secure storage and precautions when communicating intercepted communications or secondary data.[164b] Section 152 requires "selection for examination" to be necessary for an operational purpose (which, as stated, may itself be considered necessary on the basis of national security, preventing/detecting serious crime or economic wellbeing related to national security: s 138(1)(d)(ii)), necessary and proportionate in all the circumstances and that the criteria used for selection must not be referable to an individual known (or believed) to be in the British Islands if the purpose is to identify communications sent to/from that person (without a targeted examination warrant under Part 2 Chapter 1).[165] A knowing and deliberate breach of s 152 is an offence: s 155. However, as explained in paragraph 110(6) above, as a matter of construction this does not prevent disclosure

[164b] The purported requirements in Bulk Interception CoP [9.15]–[9.23] in relation to dissemination, copying, storage and destruction of material obtained under interception warrants do not materially add to the statutory provisions themselves because they are: vague, general and subjective (for example, [9.24] states that retention periods "*should normally be no longer than two years*"); and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[165] This is, broadly, the effect of ss 152(3)–(4). This prohibition on the use of criteria referable to an individual in the British Islands does not apply, for five working days, where the person (1) enters the British Islands or (2) is found to be in the British Islands: s 152(5)–(7). Bulk Interception CoP [6.66] and [6.79] state erroneously that targeted interception warrants must be sought in wider circumstances than is in fact the case. Both provision say that a targeted examination warrant must be obtained where criteria referable to an individual known to be in the British Islands are used for selection for examination, but they fail to say that this requirement applies only where, in addition, the purpose of the use of the factors is to identify communications sent to/from such a person.

or examination (~~rather than~~that occurs without selection for examination) of intercepted material. In any case, as stated, any restriction by reference to operational purposes is nil (or limited): the operational purposes together comprise all purposes for which selection for examination under any bulk interception warrant may be necessary at any time (and all operational purposes will in general be included in each bulk interception warrant).[165a] In addition, these safeguards can be disapplied altogether where intercept material is given to overseas authorities (ss 150(8), 151(2)(a)). The safeguards may also be disapplied where communications that are intercepted are retained under Part 7 (s 225(4)–(6)). ~~In any case, so far as Liberty is aware, there are no such arrangements in force.~~

114. **Circumstances of destruction:** Although a bulk interception warrant may be issued only on the grounds of national security (or national security and preventing and detecting serious crime or economic well-being linked to national security), under s 150(5)–(6) material obtained under the warrant can be retained (i) where it is "*necessary*" or "*likely to become necessary*" and (ii) this may be on the basis of any of those grounds (and, in addition, the grounds in s 150(3)(b)–(e)). Accordingly, information may be retained for different purposes from those for which it was initially collected. In addition, even if

[165a] In addition, the purported requirement to retain documentation "*outlining why*" selection for examination is necessary and proportionate and necessary for an operational purpose (and why any collateral intrusion is considered proportionate) in Bulk Interception CoP [6.74] does not increase the certainty of the access procedure because: no detail is provided as to the extent of any justification (for example, on its face it allows selection from a drop-down box of options); and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Further, the purported requirement in Bulk Interception CoP [6.74] that systems should not allow access to content or data unless such documentation has been created "*to the extent possible*" does not increase the certainty of the access procedure because it is: optional, in that it applies only to the extent possible; and in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements in Bulk Interception CoP [6.73] that only authorised persons who receive regular mandatory training regarding the provisions of the Act, s 152 and necessity/proportionality, specifically to direct authorised persons to the statutory safeguards, and to security clear all authorised persons do not meaningfully add to the certainty of the access procedure because: they are vague (so it is not possible to conclude that they are meaningful requirements); and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Further, the purported requirements in Bulk Interception CoP [6.75]–[6.76] that authorised persons are granted access "*only for defined periods of time*", after "*appropriate*" training and only where it is necessary for them to have access, and that periodic audits be undertaken, do not increase the certainty of the access procedure because: they are vague and general and, in consequence, do not impose any real limits on what may occur (for example, no maximum period of time for access or means by which it may be worked out is specified, and no frequency requirement for audits nor the person who is to audit is laid down); and in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

arrangements exist under s 150(5) for the destruction of "*every copy made of any of that material*" once there are no longer grounds under s 150(6) for retaining it:

(1) ~~This~~Section 150(5) appears to require only that "copies", and not the "material" itself (that is, the original interception material), are destroyed, given the definition of "copy" in s 150(9) and the distinction s 150 draws between the "material" and a "copy" of it. Accordingly, there appears not to be any requirement to destroy the original interception material;

(2) In any event, the nature of bulk interception means that irrelevant data will inevitably be retained~~be destroyed only if and when it is examined~~. There is no statutory limit on the retention of unselected intercept material. ~~It is possible to know whether there are grounds for retaining intercept material under s 150(6) only by examining the material.~~ In consequence, bulk interception warrants will inevitably result in "*the automatic storage of clearly irrelevant data*", which the Grand Chamber in *Zakharov* held "*cannot be considered justified under Article 8*";[166] and

(3) Further, these safeguards may be disapplied where communications that are intercepted are retained under Part 7 (s 225(4)–(6)) or provided to any overseas authorities (ss 150(7)–(8), 151(2)).

115. **Notification:** The IPCr has general responsibilities for reviewing the operation of the Act under Part 8 (especially ss 229, 233, 235). However, the Act does not require notification of surveillance after it has ended and is possible without jeopardising the purpose for which it occurred. The Act requires that the IPCr notify a person:

(1) only of a "*relevant error*", that is, an error in comply with a requirement existing under the Act and which is identified in a Schedule 7 code of practice (s 231(9));[166a]

---

166 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [255].

166a Bulk Interception CoP [10.12]–[10.14] defines relevant error (relevantly to bulk interception warrants) as one that occurs (1) only after interception/obtaining of secondary data has commenced or, if a warrant authorises selection for examination, only after selection for examination has commenced and (2) is interception of communications without lawful authority, obtaining of secondary data not in accordance with a bulk interception warrant, or a failure to adhere to the restrictions on use or disclosure under ss 150–154. Bulk Interception CoP [10.15] provides illustrative examples. Bulk Interception CoP [10.25] excludes from "relevant errors" situations where an intelligence agency was provided with a communications address and

(2) only where the error is a "*serious error*", that is, where the error has caused the person "*serious prejudice*" — a breach of the ECHR is expressly not sufficient for that purpose (s 231(2)–(3)); and

(3) only if notification is "*in the public interest*" (s 231(1), (4)),

and not otherwise (s 231(7)). Requirements for notification are thus very limited, and the executive's discretion in giving them extensive.

116. **Remedies:** Although the IPT will have jurisdiction in relation to complaints about conduct under the Act (RIPA s 65 and s 243 of the Act), as set out in paragraph 20(4) above, the IPT's decision in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* establishes that it is now necessary to have more than an "*asserted general belief*" and for there to be more than a "*potential risk*" that an individual has been subject to surveillance in order to bring a complaint.[167] It follows that the ECtHR proceeded on what is now understood to be an incorrect basis in *Kennedy v United Kingdom* when it relied on "*the absence of any evidential burden to overcome in order to lodge an application with the IPT*".[168] That burden now looms large. Without any general notification requirement, the ability to seek a remedy before the IPT is a weak safeguard. But it is the only remedy: RIPA s 65(2).

117. For the foregoing reasons, including the very broad scope of the power and its "*strategic*" nature, as well as the foregoing deficiencies in its safeguards, the power to issue bulk interception warrants under Part 6 Chapter 1 is not "in accordance with the law" or "provided by law" and/or not "necessary in a democratic society" under Articles 8 and 10 ECHR.

---

relied on this in "*good faith*" but this turns out to be incorrect. It is therefore unclear whether interception without lawful authority includes the situation where there is a warrant ostensibly authorising the interception but the interception is nonetheless unlawful (for example, it is disproportionate in all the circumstances). Bulk Interception CoP [10.22] states that there is no duty under s 231(1) to report errors by a telecommunications operator to the IPCr (even if otherwise within the definition of a "relevant error") because they are not errors "*by a public authority*" under s 231(9). This appears to be wrong in law: whenever they are discharging functions under the Act a telecommunications operator is acting as the agent of the intercepting authority, and this interpretation would undermine the efficacy of s 231. If it is correct, it is a further and significant limit on the error reporting regime. The provision in Bulk Interception CoP [10.22] that such errors should in any case be reported is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

167 [2016] UKIPTrib15165-CH [45]–[47]; see also [12].

168 *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [190].

(c) ECHR Articles 8 and 10 and journalistic protections

118. Section 154 provides that, if an intercepted communication that is retained contains "*confidential journalistic material*" (as defined in s 264), the addressee of the warrant must inform the IPCr as soon as reasonably practicable. Chapter 6 Part 1 therefore fails to provide adequately because (see paragraph 67 above) it does not:

(1) guarantee that any decision to intercept (examine, or continue to examine) confidential journalistic material is made by an independent body;

(2) provide for review by an independent body before interception occurs or before any (further) use is made of the confidential journalistic information; and/or

(3) before the decision to intercept, to examine or to continue to examine and use the confidential journalistic information, require an independent body to consider whether an overwhelming public interest favours (further) examination, disclosure or use of the confidential journalistic information.

118A. The Bulk Interception CoP[168a] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are required,[168b] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[168c]

[168a] Bulk Interception CoP [9.84]–[9.87].

[168b] In particular, Bulk Interception CoP [9.84] and [9.88] purport to require only that, where an authorised person intends to select for examination intercepted content in order to identify or confirm the identity of a journalistic source or which is believed to be confidential journalistic material (and no targeted examination warrant is required), a senior official is notified. These paragraphs state that the senior official must not be a member of the intercepting authority, but they do not require them to be independent of the executive. Further, these paragraphs do not purport to impose a requirement that an overwhelming public interest favours (further) examination, disclosure or use of the confidential journalistic information. All that the senior official must decide is whether the intercepting agency has arrangements in place for the handling, retention, use and destruction of communications that identify journalistic sources or contain confidential journalistic material.

[168c] This is so in particular in relation the purported prohibition in Bulk Interception CoP [9.84] and [9.88] on the authorised person selecting for examination content in order to identify or confirm the identity of a journalistic source or which is believed to be confidential journalistic material until the senior official has authorised it.

(d) ECHR Articles 8 and 10 and lawyer–client communications

119. Section 153 makes some provision for protecting legally privileged communications. However, these protections are inadequate to comply with the requirements under ECHR Articles 8 and 10 (as set out in paragraph 71 above) in that they:

(1) do not apply to all lawyer–client communications but, instead, only to those items that are actually "*subject to legal privilege*" (s 153(1)) or which would be but are made with the intention of furthering a criminal purpose (s 153(6));

(2) do not provide for who is to determine whether communications are (or are likely to be) legally privileged and, in any case, do not require the determination to be made by an independent person (under s 153, there is no separate requirement to consider whether privilege applies but, in any case, it is a "*senior official acting on behalf of the Secretary of State*",[169] who is not independent, that approves selection for examination of potentially privileged material and, in addition, the person who informs the IPCr of the retention of privileged items under s 153(9) is not independent);

(3) do not require an assessment of whether a communication is subject to strengthened protection under Articles 8 and 10 in all circumstances before it is intercepted and do not require this in all circumstances before it is used (instead, s 153(1) requires approval of selection for examination by a senior official only where the purpose of use of certain criteria is to identify items subject to legal privilege[170] or their use is "*likely to identify such items*" — where privileged items are otherwise selected for examination (for example, unexpectedly or where this was not likely), s 153(9) requires that the IPCr be informed as soon as is reasonably practicable but does not prevent any use of the item until the IPCr decides whether it should be destroyed or conditions should attach to its use under s 153(11)–(14)); and/or

(4) fail to ensure proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations except where a purpose of selection

---

169 Section 157(1) defines "*senior official*" as "*a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service*".

170 Or where, under s 153(6), a purpose of use of the criterion is to identify communications that would be subject to legal privilege if they were not made to further a criminal purpose, although the senior official must in that case consider under s 153(8) this to have been likely.

for examination is to identify items subject to legal privilege (only in this situation does s 153 require the designated senior official to have any regard to "*the public interest in the confidentiality of items subject to legal privilege*" or whether there are "*exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria*": see ss 153(3), (4)(b) and compare s 153(4)(a), (6) and (12)).

119A. The Bulk Interception CoP[170a] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are required,[170b] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[170c]

(e) ECHR Articles 8 and 10 with Article 14: Discrimination

119B. Section 150(1) and 152 have the effect that, where material obtained is selected for examination, if criteria for selection are used that are referable to an individual known to be in the British Islands and the purpose of using those criteria is to identify the content of communications sent by or intended for that individual, a targeted interception warrant under Part 2 of the Act (or a five-day temporary authorisation) must be obtained to authorise the selection for examination. This affords persons known to be in the British Islands additional safeguards.

119C. This is effected as follows:

[170a] Bulk Interception CoP [9.59]–[9.73].

[170b] In particular, the Bulk Interception CoP does not: (1) provide for who is to determine whether communications are (likely to be) lawyer–client communications or require this to be determined by an independent person (but, in relation to targeted and thematic warrants, provides only for consultation of a legal adviser within the interception authority where there is doubt about privilege: Bulk Interception CoP [9.50]); (2) require an assessment of whether a lawyer–client communication is subject to strengthened protection under Articles 8 and 10 ECHR in all circumstances before it is obtained, selected for examination or further used (instead, only where privileged communications are likely to be obtained by selection for examination or it is the purpose of selection for examination to obtain them, and not before any further use: see Bulk Interception CoP [9.59]–[9.61]); (3) require proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations where they are obtained, selected for examination or used (save where it is the purpose of selection for examination to obtain privileged communications, in which case the issuing authority must be satisfied that there are "*exceptional and compelling circumstances*" that make the warrant necessary: Bulk Interception CoP [9.52], [9.54]).

[170c] This applies in particular to the purported requirement in Bulk Interception CoP [9.62]–[9.64] to assume that s 194 applies where a lawyer acting a professional capacity is the subject of a targeted examination warrant or subject of examination.

(1) Section 150(1)(b) requires the Secretary of State to ensure for every bulk interception warrant that "*arrangements are in force for securing*" that "*the requirements of s 152 are met in relation to the intercepted content or secondary data obtained under the warrant*".

(2) Section 152(1)(c) and (3) makes one of the conditions in s 152 that selection for examination does not breach and is not considered to breach the prohibition in s 152(4) or, if it does, it is authorised by a targeted examination warrant under Part 2 Chapter 1 (see s 154(3)(a)–(c)).

(3) Section 152(4) prohibits the "*selection for examination*" of intercepted content where, whether or not the identity of the person is known:

> "(a) any criteria used for the selection of the intercepted content for examination are referable to an individual known to be in the British Islands at that time, and
>
> (b) the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual."

(4) Section 152(3)(d) and (5) permits a breach of the prohibition in s 152(4) in addition, without a Part 2 targeted examination warrant, where:

(a) criteria referable to an individual are being used in circumstances where this does not breach the prohibition or is considered not to breach the prohibition;

(b) it appears to the person to whom the warrant is addressed that there has been a "*relevant change in circumstances*", namely, an individual has entered the British Islands or a belief by the person to whom the warrant was addressed that the individual was outside the British Islands was in fact mistaken (s 152(6));

(c) a senior officer has given a written authorisation to examine the relevant content; and

(d) the selection for examination is made before the end of the "*permitted period*", namely, the fifth working day after the time when it appeared that there had been a relevant change in circumstances (s 152(7)).

Where this occurs, the Secretary of State must be notified: s 152(8).

119D. A targeted examination warrant authorises selection for examination of content intercepted under a bulk interception warrant: s 15(3). The issue of a targeted examination warrant requires in particular:

(1) consideration by the Secretary of State personally of whether the selection for examination authorised is necessary and proportionate (ss 19(2), 20(2), 30(1));

(2) authorisation (or in urgent cases review within five days) by a Judicial Commissioner of the Secretary of State's decision to issue the warrant, applying a judicial review standard (ss 19(2)(d), 23–24); and

(3) where a purpose of the warrant is to select for examination confidential journalistic material or to identify or confirm a source of journalistic information, that the application says this and is granted only where the arrangements under s 150 include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material (ss 28(1)(b)(ii), (2), (3) and 29).

119E. Where a person is not (believed to be) in the British Islands, there is no restriction on "selection for examination" of content by a criterion referable to that person. There is no requirement to obtain a targeted examination warrant (or a temporary authorisation) in these cases.

119F. As set out in paragraphs 71F–71K above, this constitutes discrimination on the basis of nationality, national origin and/or residence. As set out in paragraphs 71L–71N above, it is for the Defendants to seek to justify this discrimination but, as set out above, no credible justification appears to exist.

(2) Incompatibility with EU law

(a) General and indiscriminate retention of content of communications

120. Due to its breadth and the absence of provisions that **require** limitations on the scope of bulk interception warrants, Part 6 Chapter 1 constitutes a general and indiscriminate regime of retention and access by the state. Its provisions do not require a warrant to be

any narrower than a direction under Telecommunications Act 1984 s 94, which was held in *PI* at [80]–[82] to be a regime of general and indiscriminate retention and transmission to the state. Accordingly, Part 6 Chapter 1 is ~~Bulk interception warrants are~~ incompatible with EU law on each of the following alternative bases:

(1) Bulk interception warrants may be issued "in the interests of national security", whether or not on other grounds (ss 138(1)(b), (2)). If and insofar as this purpose is any wider than ~~They are not limited to~~ the purpose of ~~fighting serious crime[171] or, alternatively, to~~ preventing the most serious threats to national security (as defined in *PI* and *La Quadrature*), it is incompatible with EU law or, alternatively, it must be construed as so limited to ensure that it is compatible with EU law[171a] (see paragraph 96B above). To the extent to which "the interests of national security" extend beyond these matters, the provisions enable the issue of warrants incapable of justification as strictly necessary (see paragraphs 91–92 and 95–96B above).

(2) ~~The power to issue bulk interception warrants is a power indiscriminately and generally to retain the content of communications., and therefore~~ In addition, Part 6 Chapter 1 permits the state to retain and access content and/or secondary data (after it has been initially obtained) **other than** for the purpose of preventing the most serious threats to national security. This occurs where an operational purpose (for which content and secondary data may be selected for examination) is included in a warrant but is not itself referable to "*the interests of national security*", and is instead referable to the purpose of preventing and detecting serious crime (the "**serious crime purpose**") or to the interests of the economic wellbeing of the United Kingdom insofar as relevant to national security (the "**economic purpose**"): see ss 136(4), 138(1)(d), (2), 142(3), 152(1)(a), (2). To that extent the regime for bulk interception warrants is incompatible with EU law, as it constitutes a regime

---

~~[171] The CJEU counts terrorism as a serious crime: Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [103]. Although a bulk interception warrant may be issued for the purpose of "preventing or detecting serious crime" (if it is also in the interests of national security), the Act permits an interference for a purpose that is not capable of justification to the extent that the extensive definition of "serious crime" in section 263(1) includes crime that is not "serious" within the meaning of the judgment in *Watson*.~~

[171a] See Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* ECLI:EU:C:1990:395 [9].

of general and indiscriminate retention and access other than for the purpose of preventing the most serious threats to national security. Further, it does not limit the content and secondary data obtained and retained, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period, to what is strictly necessary (see paragraphs 95–96B above).

~~(a) affects the essence of the rights under Articles 7 and 8 (see paragraphs 93–94 above); and/or~~

~~(b) does not limit the content obtained, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period, to what is strictly necessary (see paragraphs 95–96 above).~~

(3) Insofar as Part 6 Chapter 1 (read with other provisions of the Act or subordinate legislation) permits CSPs and/or the state to carry out automated processing of data, it does not contain requirements that the model or criteria be specific and reliable, non-discriminatory (including that they are not based on sensitive matters in isolation) and regularly re-examined or that any positive result is individually reviewed before action adversely affecting an individual is taken, as set out in paragraph 102B above.

(b) Non-compliance with further Watson requirements

121. Further or alternatively, insofar as Part 6 Chapter 1 permits content and/or secondary data to be accessed and/or retained and/or otherwise processed under a bulk interception warrant **other than** for the purpose of preventing the most serious threats to national security (or for operational purposes referable to those other purposes), ~~T~~the power to issue bulk ~~acquisition~~ interception warrants fails to comply with the *Watson* requirements in each of the following alternative respects, namely, that it:

~~(1) is not strictly limited to defined and precise offences (nor even to preventing serious crime);~~

~~(2) does not ensure that continued access to data (or its retention) is connected to the objective pursued or depends on a link between continued access/retention and preventing serious crime (alternatively, a serious threat to national security);~~

~~(3) does not, as a general rule, limit government's access to data of individuals suspected of planning, committing, having committed or otherwise been implicated in serious crime (allowing access to the data of other persons only in a specific case and to protect vital national security, defence or public security interests);~~

~~(4) does not require a reasoned application from a national authority to request interception or access;~~

(5) does not require judicial or independent approval each time data is accessed, on the basis of a reasoned application from a national authority to request interception or access (save insofar as a targeted examination warrant is required to access data);

(6) does not require notification of any person affected as soon as that notification is no longer liable to jeopardise investigations being undertaken; and/or

(7) does not require data to be retained in the EU (and section 151 permits data to be provided to "*overseas authorities*" and further allows the disapplication of all retention and disclosure safeguards under Chapter 6 Part 1 in those circumstances).~~;~~

~~(8) does not require providers of electronic communications services to guarantee a particularly high level of protection (as s 150(4) requires only arrangements for storage in a secure manner, rather than a high level of protection);~~

~~(9) does not impose definitive retention periods or impose or require retention periods to be based on objective criteria or adapted depending on the usefulness of material obtained (see s 150(5)–(6)); and/or~~

~~(10) it (and the provisions in Part 8) do not require consideration by an independent authority specifically directed to compliance with the level of data protection required by EU law.~~

(ba) Non-compliance in respect of all purposes with the CFR requirements for sufficient and detailed safeguards equivalent to those under the ECHR

121A. Further or alternatively, Part 6 Chapter 1, in respect of all purposes for which content and secondary data may be obtained, retained, used and/or otherwise processed, does not comply with the requirements of ECHR Articles 8 and 10 for secret surveillance regimes as set out in paragraphs 108–117 above (and further in the Claimant's Skeleton Argument dated 10 May 2019 before the Divisional Court and the Skeleton Argument of National Union of Journalists dated 10 May 2019). As CFR Articles 7, 8 and 11 provide at least equivalent protection, Part 6 Chapter 1 is also incompatible with those provisions and accordingly incompatible with EU law.

(c) CFR Articles 7 and 11 and journalistic protection / lawyer–client communications

122. Liberty repeats paragraphs 118 and 119 above by reference to CFR Articles 7 and 11.

~~*(d) Article 18 TFEU and Article 21 CFR: Discrimination*~~

~~122A. Liberty repeats paragraphs 119B–119F above by reference to Article 18 TFEU and Article 21 CFR (see also paragraph 106A above).~~

E GROUNDS OF CHALLENGE: BULK ACQUISITION (PART 6 CHAPTER 2)

123. A brief overview of Part 6 Chapter 2 is at paragraph 18(2) above. It permits the issue of bulk acquisition warrants, which, in broad summary:

(1) May authorise or require any one or more of: (i) requiring a telecommunications operator to disclose any communications data (broadly, data about communications not including content)[172] in its possession and/or to obtain any communications data it is capable of obtaining and disclose this; (ii) the "selection for examination" of communications data obtained under the warrant; and/or (iii) the disclosure ~~to~~of communications data obtained under the warrant to its addressee;

[172] See above n 8.

(2) May be issued by the Secretary of State where considered necessary and proportionate in the interests of national security (or national security and other interests)[173] (s 158(1)) to the head of an intelligence service (s 161(2)); and

(3) Where they authorise "*selection for examination*" of intercepted communications data, must specify the operational purposes for which selection for examination of intercepted communications data is or may be necessary (ss 158(1)(c), 161(3)–(11)) — these are purposes maintained in a list by the heads of the intelligence services, which must be specified in a greater level of detail than "*the interests of national security*", for which selection for examination may be necessary.

(1) Incompatibility with ECHR

(a) Absence of individual targeting and reasonable suspicion

124. The power to issue bulk acquisition warrants is incompatible with Articles 8 and 10 ECHR because these warrants are not:

(1) limited by reference to an individual/set of premises ~~(or an individual operation or investigation)~~; and/or

(2) alternatively, permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

124A. Bulk CD CoP [3.5] makes clear that the Defendants consider (correctly) that the power to issue bulk acquisition warrants is not limited in those ways. It states that bulk acquisition "*is an intelligence gathering capability*" and contrasts this to targeted acquisition, which it describes as "*primarily an investigative tool that is used to acquire data in relation to specific investigations*".

(b) Consideration of critical factors

125. Further or alternatively, the power to issue bulk acquisition warrants is incompatible with Articles 8 and 10 ECHR because it lacks sufficient safeguards, detail and clarity as to

[173] Preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom insofar as those interests are relevant to the interests of national security (s 158(2)).

each of the critical features (and, further, the critical features taken together) in the following respects:

126. **Scope of application:** The scope of and level of discretion conferred by the bulk acquisition warrant provisions is wide. They too grant the "*almost unlimited degree of discretion*" and expressly enable the "*strategic, large-scale interception*", albeit of communications data rather than content, which *Zakharov* and *Szabó* regard as concerning.[174] Communications data contains and enables the State to ascertain substantial information about an individual, in some cases as much information as would be apparent from the content itself; as the CJEU has said in considering analogous provisions of the CFR to Articles 8 and 10 ECHR: "*those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.*"[175]

(1) As stated, bulk acquisition warrants are not limited by reference to an individual or~~,~~ set of premises~~, a particular operation or a particular investigation~~, nor do they require any factual suspicion of a particular person (even when examining communications data obtained).

(2) There is no requirement that the communications data acquired and examined is:

(a) of a certain kind;

(b) that of certain people or groups of people; or

(c) in some way geographically limited.

The discretion to acquire is in that sense wider than those the ECtHR examined in *Kennedy v United Kingdom*, *Liberty v United Kingdom* (as there is no limit to overseas communications) and *Weber and Saravia v Germany* (as there is no limit

[174] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [248]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [69].

[175] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238 [27].

to overseas communications, nor any enumerated list of serious crimes justifying the obtaining and examination of communications data).

(3) Further, the concept of "*communications data*" is not clearly defined in s 261 of the Act. Section 261(5) provides that "*communications data*" excludes "*content*", and s 261(6) defines "content" as any element of a communication (or attached/associated data) that "*reveals anything of what might reasonably be considered to be the meaning (if any) of that communication*" (subject to further exclusions). It is therefore unclear whether, for example, a picture or video would be considered to be "*content*" or does not reveal meaning, so is merely "*communications data*" and therefore subject to acquisition~~interception~~ under Part 6 Chapter 2.

(4) Liberty repeats paragraph 110(3) above: the power to issue a warrant that either permits or requires the obtaining or the examination of communications data creates further executive discretion;

(5) Liberty repeats paragraph 110(5) above: the requirements that bulk acquisition warrants be necessary and proportionate in the interests of national security ~~is~~are a weak constraint and create~~s~~ broad executive discretion. Bulk CD CoP [3.5] confirms that this understanding accords with the Defendants' own view of the scope of the power. It explains that bulk interception may in principle entail the acquisition of "*all communications data generated by a particular telecommunications operator*".

(6) Liberty repeats paragraph 110(6) above: operational purposes do not limit the initial obtaining of communications data (as they apply only at the point of selection for examination (see ss 158(1)(c) and 161(3)–(4))); operational purposes may be included in a warrant where "selection for examination" for the operational purpose is considered necessary for **any** of national security, preventing and detecting serious crime or economic wellbeing insofar as it relates to national security, not necessarily just for national security (s 158(1)(c)(ii));[175a] they do little to circumscribe examination because (i) as a matter of construction s 172 does not prevent all examination or disclosure of retained or acquired communications data,

[175a] See Bulk CD CoP [4.8].

but only "selection for examination" (and the latter is not necessary for the former to occur) and (ii) in any case, warrants may (and will — see ~~paragraph 110(6) above~~the Bulk CD CoP)[175b] contain all operational purposes (as s 161(5) expressly permits) which together constitute the universe of purposes for which communications data may be selected for examination at the time (see s 161(4) and Bulk CD CoP [6.3]–[6.4]), under s 161(7) operational purposes need only be specified "*in a greater level of detail*" than those in s 151(1)(a) or (2) (and this is an undemanding standard),[175c] and operational purposes are not required to be published, so in practice they do not effectively limit the purposes for which communications data can be selected for examination. (If the operational purposes are not published, neither their existence nor their content may be taken into account in assessing the critical features: see paragraphs 45–46B above.)

127. **Duration:** The duration of bulk interception warrants is six months, although they are subject to renewal (ss 162–3). A warrant must be cancelled where the Secretary of State or a senior official considers it no longer necessary or proportionate (s 167(2)). However, there is no statutory duty upon either the Secretary of State or a senior official to keep bulk acquisition warrants under review.[175d]

128. **Authorisation procedure:** Liberty repeats paragraph 112 above: a Judicial Commissioner approves the warrant and reviews the Secretary of State's conclusions on necessity/proportionality (ss 158(1)(e), 159), but: (i) the Judicial Commissioner applies only a judicial review standard without reasons for/opposition to the decision

---

[175b] Bulk CD CoP [6.10]: "*Other than in exceptional circumstances, it will always be necessary for a bulk acquisition warrant to require the full range of operational purposes to be specified in relation to the selection for examination of data obtained under the warrant.*"

[175c] The purported additional requirements in Bulk CD CoP [6.6] that operational purposes must "*describe a clear requirement*" and "*contain sufficient detail to satisfy the Secretary of State that acquired data data may only be selected for examination for specific reasons*" add nothing because: they are vague and subjective (and gloss s 161(7)); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[175d] The purported requirement upon intercepting authorities (not the Secretary of State) to keep warrants under review in Bulk CD CoP [5.18] does not contribute to the certainty of the duration of a warrant because: it does not state who (which person) must do this, with what regularity, by what means or on the basis of what materials; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(s 159(2));[175e] (ii) an incomplete warrant may be served on someone to compel assistance in execution, so that person cannot verify authorisation/implementation (s 168(2), (5)));[175f] (iii) an operational purpose may be added to a warrant and thereafter material may be selected for examination for the new operational purpose (other than those for which selection for examination was permitted when the data was obtained) (s 164(2)(a));[175g] (iv) modifications adding/varying operational purposes have effect without Judicial Commissioner approval for five business days, there is no review of the decision to modify urgently, and non-approval does not affect the lawfulness of past actions (ss 164(5), 166); and (~~i~~v) combined warrants are permitted but not required (Schedule 8), so the approvals process may not take into consideration all interference from related but separate warrants. In addition, a TCN can require a telecommunications operator to install equipment provided by the Secretary of State to obtain or disclose communications data (see paragraph 84(1A)(c)(ii)(F) above), which may prevent the telecommunications operator from supervising whether communications data is being obtained or disclosed in accordance with a bulk acquisition warrant.

129. **Procedure for use/examination/storage/precautions when communicating:** Liberty repeats paragraph 113 above: arrangements are required that create some safeguards for use, examination, secure storage and precautions when communicating communications

---

[175e] Further, the purported requirement in Bulk CD CoP [4.4] that there is a review within the agency prior to an application being made does not increase the certainty of the authorisation procedure because: there is no requirement for the reviewer to be independent from the person or team seeking the authorisation; the reviewer is not empowered to prevent an application if they consider that an application is not necessary or proportionate or "selection for examination" would not be necessary for an operational purpose; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements for applications in Bulk CD CoP [4.5] do not increase the certainty of the authorisation procedure because: they do not state that an application may not be made if it does not include (a satisfactory) explanation of any of the matters referred to (and do not make any other provision for this circumstance); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The purported requirement that a Judicial Commissioner has access to the same application as the Secretary of State in Bulk CD CoP [4.13] also does not increase the certainty of the authorisation procedure because: there is no provision that a Judicial Commissioner may not approve a warrant if this is not the case; and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[175f] Bulk CD CoP [4.19] and [7.3] confirms that telecommunications operators will not be given entire warrants, in that it states that it is "*unlikely*" that telecommunications operators will receive a copy of the operational purposes specified in the warrant and further states that part only of a warrant may be given to a telecommunications operator. This makes it hard or impossible for a telecommunications operator to exercise supervision over whether retention and acquisition are in accordance with a warrant.

[175g] As stated in Bulk CD CoP [5.9].

data and selection for examination must be necessary for an operational purpose and proportionate (ss 171–3), though there is no restriction on selecting using criteria referable to individuals in the British Islands. However: (i) the restrictions in ss 172–3 do not prevent all examination (rather than selection for examination — see paragraph 126(6) above); (ii) any restriction by reference to operational purposes is nil (or limited) because the operational purposes together comprise all purposes for which selection for examination under any bulk acquisition warrant may be necessary at any time (and all operational purposes will in general be included in each bulk acquisition warrant);[175h] and (iii) the safeguards may be disapplied when communications data is provided to overseas authorities (s 171(7)–(9))~~; and (iii) no arrangements under s 171 are in force in any case~~.

130. **Circumstances of destruction:** Liberty repeats paragraph 114 above: a warrant can be issued only in the interests of national security (or national security and preventing and detecting serious crime or economic well-being linked to national security) but material can be retained where (i) necessary or likely to become necessary (ii) on any of those grounds (s 171(5)–(6)) and, in addition, the grounds in s 171(3)(b)–(f) (so information may be retained for different purposes than those for which it was initially collected); the arrangements s 171(5) describes apparently do not require destruction of original

[175h] In addition, the purported requirement to retain documentation "*outlining why*" selection for examination is necessary and proportionate and necessary for an operational purpose in Bulk CD CoP [6.15] does not increase the certainty of the access procedure because: no detail is provided as to the extent of any justification (for example, on its face it allows selection from a drop-down box of options); there is no requirement that systems should not allow access to data unless the relevant documentation has been created; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements in Bulk CD CoP [9.3], [9.5] and [9.7]–[9.9] and [9.13] that only security-cleared persons should be able to access retained data, data should be held so that non-security-cleared persons cannot access it, that the number of persons to whom data is disclosed (and the extent of disclosure) should be "*limited to the minimum that is necessary*", and that all copies, extracts and summaries of data should be "*scheduled for destruction as soon as possible*" once it is no longer needed for any other authorised purposes do not meaningfully add to the certainty of the access procedure because: they are vague (so it is not possible to conclude that they are meaningful requirements) and subjective standards (for example, no maximum period of time for access or means by which it may be worked out or guideline on this is specified); and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Further, the purported requirement in Bulk CD CoP [6.16] that periodic audits be undertaken does not increase the certainty of the access procedure because: this is vague and general and, in consequence, does not impose any real limits on what may occur (for example, no frequency requirement for audits nor the person who is to audit is set out); and in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

intercept "material", only any "copies" (see s 171(9)); and it is inevitable that clearly irrelevant communications data will be retained.

131. **Notification and remedies:** Notification is very rarely required under the Act[175i] and, where required, in the IPCr's discretion, and the ability to apply to the IPT for investigation is a far weaker safeguard than previously thought (see paragraphs 115–116 above).

132. For the foregoing reasons, the power to issue bulk acquisition warrants under Part 6 Chapter 2 is not "in accordance with the law" or "provided by law" and/or not "necessary in a democratic society" under Articles 8 and 10 ECHR.

(c) ECHR Articles 8 and 10 and journalistic protections

133. Part 6 Chapter 2 makes no express provision in relation to journalistic material at all. Accordingly, it fails to comply with any of the mandatory requirements under ECHR Articles 8 and 10, namely, it does not:

(1) guarantee that any decision to obtain (examine, or continue to examine) communications data revealing any journalistic material[176] is made by an independent body;

[175i] Bulk CD CoP [10.9]–[10.12] defines relevant error (relevantly to bulk acquisition warrants) as one that occurs (1) only after acquisition of data has been initiated and (2) is (a) bulk acquisition of communications data without lawful authority and where data has been diverted or recorded so as to be made available to a person subsequently or (b) a failure to adhere to the restrictions on use or disclosure under ss 171–172. This definition is unclear (in particular, the requirement for diversion or recording so as to make data available "subsequently"), and thereby limits the effectiveness of the reporting regime. It is also unclear whether acquisition without lawful authority includes the situation where there is a warrant ostensibly authorising the acquisition but the acquisition is nonetheless unlawful (for example, it is disproportionate in all the circumstances). Bulk CD CoP [10.13] provides illustrative examples. Bulk CD CoP [10.20] states that there is no duty under s 231(1) to report errors by a telecommunications operator to the IPCr (even if otherwise within the definition of a "relevant error") because they are not errors "*by a public authority*" under s 231(9). This appears to be wrong in law: whenever they are discharging functions under the Act a telecommunications operator is acting as the agent of the intercepting authority, and this interpretation would undermine the efficacy of s 231. If it is correct, it is a further and significant limit on the error reporting regime. The provision in Bulk CD CoP [10.20] that such errors should in any case be reported is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[176] For example, through the timing of contact between a person and a journalist (where the timing of the appearance of a story is known).

(2) provide for review by an independent body before obtaining of communications data occurs or before any (further) use is made of the communications data that reveals any journalistic material; and/or

(3) before the decision is made to obtain communications data, to examine or to continue to examine and use communications data that reveals any journalistic material, require an independent body to consider whether an overwhelming public interest favours (further) examination, disclosure or use of the journalistic information revealed by the communications data.

133A. The Bulk Acquisition CoP[176a] cannot and does not cure these defects. The relevant provisions do not address these requirements at all, do not purport to effect the safeguards that are required,[176b] and/or are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(d) ECHR Articles 8 and 10 and lawyer–client communications

134. It is possible to ascertain the existence of and information about lawyer–client communications from communications data, for example, whether, when and for how long a lawyer and client have spoken or otherwise communicated. That information may on occasion be sensitive or confidential. Nonetheless, Part 6 Chapter 2 contains no provisions that protect communications data that would reveal anything about lawyer–client communications. Further, the Bulk CD CoP says (relevantly) only that an authorised person must consider "*additional sensitivities*" where it is "*intended or known*" that the data being selected for examination includes communications of various groups that include lawyers.[176c] Accordingly, Part 6 Chapter 2 it is incompatible with

[176a] Bulk CD CoP [6.24]–[6.31].

[176b] In particular, Bulk CD CoP [6.25] purports to require an overwhelming public interest only where communications data is selected for examination in order to identify a source of journalistic information and Bulk CD CoP [6.28]–[6.30] purport to require that a person holding the rank of Director or above approves selection for examination specifically in order to determine a journalist's source (but expressly not, where the intention is to examine the communications data of a person known to be a journalist, if it is not "*intended*" to identify a journalistic source). These paragraphs expressly permit approval by a member of the intercepting authority (not an independent person). Further, they do not purport to impose a requirement that an overwhelming public interest favours (further) examination, disclosure or use of the confidential journalistic information, save where the examination is to identify a journalistic source.

[176c] Bulk CD CoP [6.23]. In addition, Bulk CD CoP [6.22] states that "*special consideration*" must be given to necessity and proportionality where there are "*any such circumstances*" (which appears to refer to the

Articles 8 and 10 ECHR in that it fails to provide for any of the four requirements set out in paragraph 71 above.

(2) Incompatibility with EU law

(a) General and indiscriminate retention of ~~content of~~ communications data

135. Liberty repeats paragraph~~s~~ 120~~120(1) and 120(2)(b)~~ above: Due to its breadth and the absence of provisions that **require** limitations on the scope of bulk acquisition warrants, Part 6 Chapter 2 constitutes a general and indiscriminate regime of retention and access by the state. Its provisions do not require a warrant to be any narrower than a direction under Telecommunications Act 1984 s 94, which was held in *PI* at [80]–[82] to be a regime of general and indiscriminate retention and transmission to the state. Accordingly, Part 6 Chapter 2 is ~~bulk acquisition warrants are~~ incompatible with EU law on each of the following alternative bases~~because they are~~:

(1) Bulk acquisition warrants may be issued "in the interests of national security", whether or not on other grounds (ss 158(1)(a), (2)). If and insofar as this purpose is any wider than ~~not limited to~~ the purpose of ~~fighting serious crime or, alternatively, to~~ preventing the most serious threats to national security (as defined in *PI* and *La Quadrature*), it is incompatible with EU law or, alternatively, it must be construed as so limited to ensure that it is compatible with EU law[176d] (see paragraph 96B above). To the extent to which "the interests of national security" extend beyond these matters, the provisions enable, ~~so as to allow~~ the issue of a warrant for purposes that are not capable of justifying an interference with Article 7 and 8 rights (see paragraphs 91–92 and 95–96B above).~~; and/or~~

(2) In addition, Part 6 Chapter 2 permits the state to **retain and access** communications data (after it has been initially obtained) **other than** for the purpose of preventing the most serious threats to national security. This occurs where an operational

---

circumstances listed in [6.21], which include "*legally privileged information*") that "*might lead to an unusual degree of intrusion or infringement of rights and freedoms*". This suggests that acquiring communications data that reveals legally privileged information does not always lead to an unusual degree of intrusion into privacy.

[176d] See Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* ECLI:EU:C:1990:395 [9].

purpose (for which communications data may be selected for examination) is included in a warrant but is not itself referable to "*the interests of national security*", and is instead referable to the serious crime purpose or to the economic purpose: see ss 158(1)(a), (2), 161(3), 172(1)(a), (2). To that extent the regime for bulk acquisition warrants is incompatible with EU law, as it constitutes a regime of general and indiscriminate retention and access other than for the purpose of preventing the most serious threats to national security. Further, ~~alternatively,~~ the communications data obtained is not limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, so as to permit only what is strictly necessary (see paragraphs 95–96B above).

(3) Insofar as Part 6 Chapter 2 (read with other provisions of the Act or subordinate legislation) permits CSPs and/or the state to carry out automated processing of data, it does not contain requirements that the model or criteria be specific and reliable, non-discriminatory (including that they are not based on sensitive matters in isolation) and regularly re-examined or that any positive result is individually reviewed before action adversely affecting an individual is taken, as set out in paragraph 102B above.

(b) Non-compliance with further Watson requirements

136. Further or alternatively, insofar as Part 6 Chapter 2 permits communications data to be accessed and/or retained and/or otherwise processed under a bulk acquisition warrant **other than** for the purpose of preventing the most serious threats to national security (or for operational purposes referable to those other purposes), ~~T~~the power to issue bulk acquisition warrants fails to comply with the *Watson* requirements in each of the following alternative respects, namely, that it:

~~(1) is not strictly limited to defined and precise offences (nor even to preventing serious crime);~~

~~(2) does not ensure that continued access to data (or its retention) is connected to the objective pursued or depends on a link between continued access/retention and preventing serious crime (alternatively, a serious threat to national security);~~

~~(3) does not, as a general rule, limit government's access to data of individuals suspected of planning, committing, having committed or otherwise been implicated in serious crime (allowing access to the data of other persons only in a specific case and to protect vital national security, defence or public security interests);~~

~~(4) does not require a reasoned application from a national authority to request interception or access;~~

(5) does not require judicial or independent approval each time data is accessed, on the basis of a reasoned application from a national authority to request acquisition or access;

(6) does not require notification of any person affected as soon as that notification is no longer liable to jeopardise investigations being undertaken; and/or

(7) does not require data to be retained in the EU (and section 171 permits data to be provided to "*overseas authorities*" and further allows the disapplication of all retention and disclosure safeguards under Chapter 6 Part 2 in those circumstances).~~;~~

~~(8) does not require providers of electronic communications services to guarantee a particularly high level of protection (as s 150(4) requires only arrangements for storage in a secure manner, rather than a high level of protection);~~

~~(9) does not impose definitive retention periods or impose or require retention periods to be based on objective criteria or adapted depending on the usefulness of material obtained (see s 150(5)–(6)); and/or~~

~~(10) it (and the provisions in Part 8) do not require consideration by an independent authority specifically directed to compliance with the level of data protection required by EU law.~~

(ba) Non-compliance in respect of all purposes with the CFR requirements for sufficient and detailed safeguards equivalent to those under the ECHR

136A. Further or alternatively, Part 6 Chapter 2, in respect of all purposes for which communications data may be obtained, retained, used and/or otherwise processed, does not comply with the requirements of ECHR Articles 8 and 10 for secret surveillance

regimes as set out in paragraphs 124–132 above (and further in the Claimant's Skeleton Argument dated 10 May 2019 before the Divisional Court and the Skeleton Argument of National Union of Journalists dated 10 May 2019). As CFR Articles 7, 8 and 11 provide at least equivalent protection, Part 6 Chapter 2 is also incompatible with those provisions and accordingly incompatible with EU law.

(c) CFR Articles 7 and 11 and journalistic protection / lawyer–client communications

137. Liberty repeats paragraphs 133 and 134 above by reference to CFR Articles 7 and 11.

F GROUNDS OF CHALLENGE: BULK HACKING (PART 6 CHAPTER 3)

138. A brief overview of Part 6 Chapter 3 is at paragraph 18(3) above. It permits the issue of bulk equipment interference (hacking) warrants, which, in broad summary:

(1) Must authorise or require the securing of "*interference*" with equipment for the purpose of obtaining "*communications*", "*equipment data*" and "*any other information*" (s 176(1)(b), (4)(a)), although this power cannot be used to intercept communications during transmission that are not stored (s 176(6)). They may, in addition, authorise or require (ii) the "*selection for examination*" of data obtained under the warrant; and/or (iii) the disclosure of anything obtained under the warrant to its addressee (s 176(4)(b));

(2) Must have as their "main" purpose one or more of (i) obtaining overseas-related communications (those sent/received by individuals outside the British Islands), (ii) obtaining overseas-related information (information of individuals outside the British Islands), or (iii) obtaining overseas related equipment data (s 176(1)(c), (3));

(3) May be issued by the Secretary of State where considered necessary and proportionate in the interests of national security (or national security and other interests)[177] (s 176(1)) to the head of an intelligence service (s 183(3)); and

[177] Preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom insofar as those interests are relevant to the interests of national security (s 178(1)(b), (2)).

(4) Where they authorise "*selection for examination*" of intercepted content, must specify the "operational purposes" for which selection for examination of intercepted content is or may be necessary (ss 138(1)(d), 142(3)–(10)) — these are purposes maintained in a list by the heads of the intelligence services, which must be specified in a greater level of detail than "*the interests of national security*", for which selection for examination may be necessary.

(1) Incompatibility with ECHR

(a) Absence of individual targeting and reasonable suspicion

139. The power to issue bulk equipment interference warrants is incompatible with Articles 8 and 10 ECHR because these warrants are not:

(1) limited by reference to an individual/set of premises ~~(or an individual operation or investigation)~~; and/or

(2) alternatively, permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

139A. Bulk EI CoP [6.5] makes clear that the Defendants consider (correctly) that the power to issue bulk equipment interference warrants is not limited in those ways. It indicates that a bulk equipment interference warrant should be issued where the Secretary of State is not "*able to foresee the extent of all of the interferences to a sufficient degree to properly and fully assess necessity and proportionality* ***at the time of issuing the warrant***" (original emphasis).

(b) Consideration of critical factors

140. Further or alternatively, the power to issue bulk equipment interference~~acquisition~~ warrants is incompatible with Articles 8 and 10 ECHR because it lacks sufficient safeguards, detail and clarity as to each of the critical features (and, further, the critical features taken together) in the following respects:

141. **Scope of application:** The scope of and level of discretion conferred by the bulk interception warrant provisions is the widest of any of the bulk powers in Part 6, because

it applies to a wider range of communications and information (potentially anything stored in an electronic device, regardless of whether it is a communication or is being transmitted/stored in a telecommunications system)[178] and a wider range of activities (any "*interference*" with "*equipment*"). It is also more a serious interference with Article 8 rights, because it applies more widely as described, it enables the retrieval of information never sent via a network (in respect of which there is an increased expectation of privacy) and interference may also extend to altering a person's data or altering their device or the way in which it functions (or other equipment), if necessary to retrieve information (s 176(5)). It creates yet further an "*unlimited degree of discretion*" and expressly is the "*strategic, large-scale interception*":[179]

(1) As stated, bulk equipment interference warrants are not limited by reference to an individual or, set of premises~~, a particular operation or a particular investigation~~, nor do they require any factual suspicion of a particular person (even when examining communications and information obtained, whether or not under a Part 5 targeted inspection warrant).[180]

(2) Liberty repeats paragraph 110(2) above: the requirement of a "*main purpose*" of obtaining overseas-related communications or information (s 176(1)(c)) permits other undefined subsidiary purposes, including intercepting intra-UK communications; the definitions of "*overseas-related communications*" and "*overseas-related information*" (in s 176(2)) make this constraint very weak in practice (because the physical locations of those whose communication and information are captured cannot be known when the warrant authorising their capture is issued); and these definitions permit capture of communications "*received by*" and information "*of*" individuals outside the British Islands, even if

---

178 However, a bulk equipment interference warrant cannot authorise the interception of communications in the course of their transmission where this would otherwise be an offence under section 3(1) of the Act: ss 176(6)–(7).

179 Cf *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [248]; *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section) [69].

180 Targeted examination warrants permit the selection for examination of material obtained under a bulk equipment interference warrant using criteria referable to an individual in or believed to be in the British Islands for the purpose of identifying "protected material" consisting of that communications sent/received by that person or private information relating to her or him: see s 193(3)(d), (4). The provisions that define targeted examination warrants are relevantly ss 101(2), 102(3) and 115(5).

the intended recipient or final person holding information (and the sender) are in the United Kingdom. The Bulk EI CoP provides no guidance on how this assessment is to be made.[180a]

(3) Liberty repeats paragraph 110(3) above: bulk equipment interference warrants permit or require interception (s 136(4)), which creates further executive discretion.

(4) Liberty repeats paragraph 110(4) above: there is no closed list of offences for which the power may be exercised, nor is the power directed exclusively to overseas communications.

(5) Liberty repeats paragraph 110(5) above: the requirement that bulk equipment interference warrants be necessary and proportionate in the interests of national security is a weak constraint and creates broad executive discretion.

(6) Liberty repeats paragraph 110(6) above: operational purposes do not limit the initial equipment interference to obtain communications or other information, as they apply only at the point of "selection for examination" (see ss 191(1)(b), 193(1)(a) and 193(2)); operational purposes may be included in a warrant where "selection for examination" for the operational purpose is necessary for **any** of national security, preventing and detecting serious crime or economic wellbeing insofar as it relates to national security, not necessarily just for national security (s 178(1)(d)(ii));[180b] operational purposes~~they~~ do little to circumscribe examination because: (i) as a matter of construction s 193 does not prevent all examination or disclosure of intercepted material, but only selection for examination (and the latter is not necessary for the former to occur); and (ii) in any case, warrants may (and will — see ~~paragraph 110(6) above~~Bulk EI CoP [6.6]–[6.7])[180c] contain all

---

[180a] Even if it did, this would not be a statutory requirement so could be departed from if there were cogent reasons to do so (see paragraph 61 above).

[180b] See Bulk EI CoP [6.16].

[180c] Bulk EI CoP [6.6]–[6.7]:

"*It is highly likely that a bulk equipment interference warrant will specify the full range of operational purposes (in accordance with section 183(6)); …*

In addition, other than in exceptional circumstances, it will always be necessary for all the operational purposes included in the central list of operational purposes maintained by the heads of the intelligence services to be specified in relation to the selection for examination of any material obtained under a bulk equipment interference warrant that is not protected material."

operational purposes for which material may be selected for examination at the time when the warrant is issued (as s 183(6) expressly permits and Bulk EI CoP [6.67] elaborates), operational purposes are only purposes for which examination **may** be necessary, operational purposes are not required to be published, and operational purposes must under s 183(8) be specified "*in a greater level of detail*" than the purposes in s 178(1)(b) or (2) (but this is an undemanding standard),[180d] so in practice operational purposes do not effectively limit the purposes for which communications data can be selected for examination. (Further, if the operational purposes are not published, neither their existence nor their content may be taken into account in assessing the critical features: see paragraphs 45–46B above.)

Accordingly, the discretion conferred is wider than in *Liberty v United Kingdom* or *Weber*, both as to the conduct it authorises and the circumstances in which it can be used. Given the extent of equipment interference, the powers conferred go well beyond those that the ECtHR has ever upheld.

142. **Duration:** The duration of bulk equipment interference warrants is six months (or, if issued urgently without Judicial Commissioner approval but later approved, five working days), although they are subject to renewal (ss 184–5). A warrant must be cancelled where the Secretary of State or a senior official considers it no longer necessary or proportionate (s 189(2)–(3)). However, there is no statutory duty upon either the Secretary of State or a senior official to keep bulk equipment interference warrants under review.[180e]

143. **Authorisation procedure:**

See also Bulk EI CoP [6.73]–[6.74].

[180d] The purported additional requirements in Bulk EI CoP [6.69] that operational purposes must "*describe a clear requirement*" and "*contain sufficient detail to satisfy the Secretary of State that material may only be selected for examination for specific reasons*" add nothing because: they are vague and subjective (and gloss s 183(8)); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[180e] The purported requirement upon intelligence agencies (not the Secretary of State) to keep warrants under review in Bulk EI CoP [6.62] does not contribute to the certainty of the duration of a warrant because: it does not state who (which person) must do this, with what regularity, by what means or on the basis of what materials; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The similar requirements in Bulk EI CoP [9.19]–[9.20] for equipment interference authorities to undertake "[r]*egular*" reviews of warrants "*as frequently as is considered necessary and proportionate*" suffer from the same vices.

(1) Liberty repeats paragraph 112 above: a Judicial Commissioner approves the warrant and reviews the Secretary of State's conclusions on necessity/proportionality (ss 178(1)(f), 179), but: (i) the Judicial Commissioner applies only a judicial review standard without reasons for/opposition to the decision (s 179(2));[180f] (ii) an incomplete warrant may be served on someone to compel assistance in execution, so that person cannot verify authorisation/implementation (s 190(2), (6)));[180g] (iii) an operational purpose may be added to a warrant and thereafter material may be selected for examination for the new operational purpose (other than those for which selection for examination was permitted when the data was obtained) (s 186(2)(a));[180h] (iv) modifications adding/varying operational purposes have effect without Judicial Commissioner approval for five business days, there is no review of the decision to modify urgently, and non-approval does not affect the lawfulness of past actions (ss 186(6), 188); and (~~i~~v) combined warrants are permitted but not required (see Schedule 8), so the approvals process may not take into consideration all interference from related but separate warrants.

(2) In addition, bulk equipment interference warrants can be issued in the first instance urgently, that is, without Judicial Commissioner approval for up to three working

---

[180f] Further, the purported requirement in Bulk EI CoP [6.12] that there is a review within the agency prior to an application being made does not increase the certainty of the authorisation procedure because: there is no requirement for the reviewer to be independent from the person or team seeking the authorisation; the reviewer is not empowered to prevent an application if they consider that an application is not necessary or proportionate or "selection for examination" would not be necessary for an operational purpose; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements for applications in Bulk EI CoP [4.25] and [6.13] do not increase the certainty of the authorisation procedure because: they do not state that an application may not be made if it does not include (a satisfactory) explanation of any of the matters referred to (and do not make any other provision for this circumstance); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The purported requirement that a Judicial Commissioner has access to the same application as the Secretary of State in Bulk EI CoP [6.23] also does not increase the certainty of the authorisation procedure because: there is no provision that a Judicial Commissioner may not approve a warrant if this is not the case; and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[180g] Bulk EI CoP [7.15]–[7.16] confirms that telecommunications operators will not be given entire warrants, in that it states part only of a warrant may be given to a telecommunications operator and states that a telecommunications operator "*will not necessarily be provided with all the information contained in the warrant*". This makes it hard or impossible for a telecommunications operator or other person to exercise supervision over whether retention and acquisition are in accordance with a warrant.

[180h] As stated in Bulk EI CoP [6.51].

days (ss 178(1)(f), 180(3)). Non-approval after the fact by the Judicial Commissioner does not affect the lawfulness of anything done before the Judicial Commissioner's decision (s 181(8)), there is no definition in the Act of "urgency"[180i] nor any review of the decision to approve urgently (s 180),[181] and non-approval by the Judicial Commissioner enlivens only a discretion of the Judicial Commissioner, rather than any requirement, to destroy or impose conditions on the use of the underlying material (s 181(3)). There is no obvious justification for an urgent bulk hacking warrant.

144. **Procedure for use/examination/storage/precautions when communicating:** Liberty repeats paragraph 113 above: arrangements are required that create some safeguards for use, examination, secure storage and precautions when communicating information or communications obtained, selection for examination must be necessary for an operational purpose (which, as stated, may itself be considered necessary on the basis of national security, preventing/detecting serious crime or economic wellbeing related to national security: s 178(1)(d)(ii)) and proportionate, and ~~that~~ criteria that are referable to an individual known ~~(or believed)~~ to be in the British Islands may not be used for selection if the purpose is to identify communications sent to/from ~~them~~the individual or "private information" relating to them (without a targeted examination warrant under Part 5) (ss 191, 193, 196).[181a] However: (i) the restrictions in ss 193 and 196 do not prevent all

---

[180i] This ambiguity is made worse by the Bulk EI CoP containing at least two differing definitions of "urgency", which themselves are confusing. Bulk EI CoP [5.67] and [6.29] state that urgency is determined by "*whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the time available to meet an operational or investigative need*" (which is vague and indeterminate), but go on to say that an urgent situation "*should fall into one or both*" of two categories, namely, "*imminent threat to life or serious harm*" and "*an intelligence-gathering or investigative opportunity with limited time to act*" (again an indeterminate category). Bulk EI CoP [5.91] states (albeit in the context of Chapter 5) that a modification "*will only be considered urgent if there is a very limited window of opportunity to act*", suggesting a different (and wider) test. In any case, these definitions are not a statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[181] *Zakharov* treated the absence of any review of whether it was appropriate to approve a warrant urgently a relevant factor showing insufficient safeguards. The ECtHR commented that urgency procedures are permissible but must provide "*sufficient safeguards to ensure that it is used sparingly and only in duly justified cases*", in particular by defining urgency so as to avoid conferring "*an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure*" (for example, by requiring an "*immediate risk*") and ensuring review of "*whether the use of the urgent procedure was justified*" and what should be done with material obtained: *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [266].

[181a] Bulk EI CoP [4.4], [5.36], [6.3], [6.9] and [6.72] state erroneously that targeted interception warrants must be sought in wider circumstances than is in fact the case. These provisions say that a targeted examination

disclosure or examination (~~rather than~~that occurs without selection for examination — see paragraph 141(6) above); (ii) any restriction by reference to operational purposes is nil (or limited) because the operational purposes together comprise all purposes for which selection for examination under any bulk hacking warrant may be necessary at any time (and all operational purposes will in general be included in each bulk hacking warrant);[181b] (iii) the safeguards may be disapplied when communications data is provided to overseas authorities (s 192); and (iii) safeguards may be disapplied where material obtained is retained under Part 7 (s 225(4)–(6))~~; and (iv) no arrangements under s 191 are in force in any case~~.

145. **Circumstances of destruction:** Liberty repeats paragraph 114 above: a warrant can be issued only in the interests of national security (or national security and preventing and detecting serious crime or economic well-being linked to national security) but material can be retained where (i) necessary or likely to become necessary (ii) on any of those grounds (s 191(5)–(6)) and, in addition, the grounds in s 191(3)(b)–(e) (so information may be retained for different purposes than those for which it was initially collected); the arrangements s 191(5) describes apparently do not require destruction of original intercept "material", but only of any "copies" (see s 191(9)); it is inevitable that clearly irrelevant communications data will be retained; and the safeguard in s 191(5) may be

---

warrant must be obtained where criteria referable to an individual known to be in the British Islands are used for selection for examination, but they fail to say that this requirement applies only where, in addition, the purpose of the use of the factors is to identify communications sent to/from such a person.

[181b] In addition, the purported requirement to retain documentation "*outlining why*" selection for examination is proportionate and necessary for an operational purpose in Bulk EI CoP [6.8] and [6.78] does not increase the certainty of the access procedure because: no detail is provided as to the extent of any justification (for example, on its face it allows selection from a drop-down box of options) save that it must consider collateral intrusion; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The purported requirements in Bulk EI CoP [9.22], [9.30] and [9.31] in relation to dissemination, copying, storage and destruction of material obtained under interception warrants do not materially add to the statutory provisions themselves because they are: vague, general and subjective (for example, [9.31] states that retention periods "*should normally be no longer than two years*"); and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Further, the purported requirements in Bulk EI CoP [6.77], [6.79]–[6.80], [9.22] and [9.28] that retained data should be held such that only security-cleared and trained persons should be able to access it, authorised persons are granted access "*only for defined periods of time*" and only where it is necessary for them to have access, and that periodic audits be undertaken do not increase the certainty of the access procedure because: they are vague and general and, in consequence, do not impose any real limits on what may occur (for example, no maximum period of time for access or means by which it may be worked out is specified, and no frequency requirement for audits nor the person who is to audit is laid down); and in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

disapplied where communications and information obtained formfrom a bulk personal dataset under Part 7 (s 225(4)–(6)) or are provided to any overseas authorities (ss 191(7)–(8), 192(2)).

146. **Notification and remedies:** Notification is very rarely required under the Act[181c] and, where required, in the IPCr's discretion, and the ability to apply to the IPT for investigation is a far weaker safeguard than previously thought (see paragraphs 115–116 above).

147. For the foregoing reasons, the power to issue equipment interference (hacking) acquisition warrants under Part 6 Chapter 3 is not "in accordance with the law" or "provided by law" and/or not "necessary in a democratic society" under Articles 8 and 10 ECHR.

(c) ECHR Articles 8 and 10 and journalistic protections

148. Part 6 Chapter 3 (s 195) makes exactly the same provision as s 154 in Part 6 Chapter 1. Accordingly, for the same reasons as set out in paragraph 118 above, it fails to comply with each of the three alternative mandatory requirements under ECHR Articles 8 and 10 in respect of protection of journalistic sources.

[181c] Bulk EI CoP [10.15]–[10.16] defines relevant error (relevantly to bulk hacking warrants) as one that occurs (1) only after equipment interference has been initiated or, where a warrant authorises selection for examination, only after selection for examination commences and (2) is (a) equipment interference without lawful authority (b) a failure to adhere to the safeguards or restrictions on disclosure under ss 191–195. This definition is unclear: in particular, it is not clear whether equipment interference without lawful authority includes the situation where there is a warrant ostensibly authorising the equipment interference but the equipment interference is nonetheless unlawful (for example, it is disproportionate in all the circumstances): see Bulk EI CoP [10.16] and fn 26. Further, Bulk EI CoP [10.27] excludes from relevant errors interception on the basis of incorrect information on which the equipment interference authority relied in good faith. These limits the effectiveness of the reporting regime. Bulk Interception CoP [10.17] provides illustrative examples. Bulk CD CoP [10.24] states that there is no duty under s 231(1) to report errors by a telecommunications operator or other person to the IPCr (even if otherwise within the definition of a "relevant error") because they are not errors "*by a public authority*" under s 231(9). This appears to be wrong in law: whenever they are discharging functions under the Act a telecommunications operator or other person is acting as the agent of the intercepting authority, and this interpretation would undermine the efficacy of s 231. If it is correct, it is a further and significant limit on the error reporting regime. The provision in Bulk CD CoP [10.24] that such errors should in any case be reported is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

148A. The Bulk EI CoP[181d] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are required,[181e] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[181f]

(d) ECHR Articles 8 and 10 and lawyer–client communications

149. Section 194 makes effectively identical provision to s 153 in Part 6 Chapter 1. Accordingly, s 194 is incompatible with Articles 8 and 10 ECHR also in each of the respects set out in paragraph 119 above.

149A. The Bulk EI CoP[181g] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are required,[181h] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[181i]

[181d] Bulk EI CoP [9.81]–[9.83].

[181e] In particular, Bulk EI CoP [9.81] and [9.83] purport to require only that, where an authorised person intends to select for examination material obtained in order to identify or confirm the identity of a journalistic source or which is believed to be confidential journalistic material (and no targeted examination warrant is required), a senior official is notified. These paragraphs state that the senior official must not be a member of the intercepting authority, but they do not require them to be independent of the executive. Further, these paragraphs do not purport to impose a requirement that an overwhelming public interest favours (further) examination, disclosure or use of the confidential journalistic information. All that the senior official must decide is whether the intercepting agency has arrangements in place for the handling, retention, use and destruction of communications that identify journalistic sources or contain confidential journalistic material.

[181f] This is so in particular in relation the purported prohibition in Bulk EI CoP [9.81] and [9.82] on the authorised person selecting for examination content in order to identify or confirm the identity of a journalistic source or which is believed to be confidential journalistic material until the senior official has authorised it.

[181g] Bulk EI CoP [9.44]–[9.47], [9.55]–[9.69].

[181h] In particular, the Bulk EI CoP does not: (1) provide for who is to determine whether communications are (likely to be) lawyer–client communications or require this to be determined by an independent person (but, in relation to targeted and thematic warrants, provides only for consultation of a legal adviser within the equipment interference authority where there is doubt about privilege: Bulk EI CoP [9.46]); (2) require an assessment of whether a lawyer–client communication is subject to strengthened protection under Articles 8 and 10 ECHR in all circumstances before it is obtained, selected for examination or further used (instead, only where privileged communications are likely to be obtained by selection for examination or it is the purpose of selection for examination to obtain them, and not before any further use: see Bulk EI CoP [9.55]–[9.56]); (3) require proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations where they are obtained, selected for examination or used (save where it is the purpose of selection for examination to obtain privileged communications, in which case the issuing authority must be satisfied that there are "*exceptional and compelling circumstances*" that make the warrant necessary: Bulk EI CoP [9.50], [9.56]).

[181i] This applies in particular to the purported requirement in Bulk EI CoP [9.58]–[9.60] to assume that s 194 applies where a lawyer acting a professional capacity is the subject of a targeted examination warrant or subject of examination.

(e) ECHR Articles 8 and 10 with Article 14: Discrimination

149B. Sections 191(1) and 193 have effect that, where material is selected for examination, if criteria for selection are used that are referable to an individual known to be in the British Islands and the purpose of using those criteria is to identify the "protected material" consisting of communications sent by or intended for that individual or "private information" relating to that individual, a targeted interception warrant under Part 5 of the Act (or a five-day temporary authorisation) must be obtained to authorise the selection for examination. This affords persons known to be in the British Islands additional safeguards.

149C. This is effected as follows:

(1) Section 191(1)(b) requires the Secretary of State to ensure for every bulk hacking warrant that "*arrangements are in force for securing*" that "*the requirements of s 193 are met in relation to* [the material obtained under the warrant]".

(2) Section 193(1)(c) and (3) makes one of the conditions in s 193 that selection for examination does not breach and is not considered to breach the prohibition in s 193(4) or, if it does, it is authorised by a targeted examination warrant under Part 2 Chapter 1 (see s 193(3)(a)–(d)).

(3) Section 193(4) prohibits the "*selection for examination*" of intercepted content where, whether or not the identity of the person is known:

> "(a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and
>
> (b) the purpose of using those criteria is to identify protected material consisting of communications sent by, or intended for, that individual or private information relating to that individual."

(4) Section 193(3)(d) and (5) permits a breach of the prohibition in s 152(4) in addition, without a Part 5 targeted examination warrant, where:

(a) criteria referable to an individual are being used in circumstances where this does not breach the prohibition or is considered not to breach the prohibition;

(b) it appears to the person to whom the warrant is addressed that there has been a "*relevant change in circumstances*", namely, an individual has entered the British Islands or a belief by the person to whom the warrant was addressed that the individual was outside the British Islands was in fact mistaken (s 193(6));

(c) a senior officer has given a written authorisation to examine the relevant content; and

(d) the selection for examination is made before the end of the "*permitted period*", namely, the fifth working day after the time when it appeared that there had been a relevant change in circumstances (s 193(7)).

Where this occurs, the Secretary of State must be notified: s 193(8).

149D. A targeted examination warrant authorises selection for examination of content intercepted under a bulk hacking warrant: s 99(9). The issue of a targeted examination warrant requires in particular:

(1) consideration by the Secretary of State personally of whether the selection for examination authorised is necessary and proportionate (ss 99(9), 102(3), 105(1));

(2) authorisation (or in urgent cases review within five days) by a Judicial Commissioner of the Secretary of State's decision to issue the warrant, applying a judicial review standard (ss 102(3)(d), 108–109); and

(3) where a purpose of the warrant is to select for examination confidential journalistic material or to identify or confirm a source of journalistic information, that the application says this and is granted only where the arrangements under s 191 include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material (ss 113(1)(b), (2)–(3) and 114).

149E. Where a person is not (believed to be) in the British Islands, there is no restriction on "selection for examination" of content by a criterion referable to that person. There is no requirement to obtain a targeted examination warrant (or a temporary authorisation) in these cases.

149F. As set out in paragraphs 71F–71K above, this constitutes discrimination on the basis of nationality, national origin and/or residence. As set out in paragraphs 71L–71N above, it is for the Defendants to seek to justify this discrimination but, as set out above, no credible justification appears to exist.

(2) Incompatibility with EU law

(a) General and indiscriminate retention of content of communications

150. Liberty repeats paragraph 120 above: Due to its breadth and the absence of provisions that **require** limitations on the scope of bulk equipment interference warrants, Part 6 Chapter 3 constitutes a general and indiscriminate regime of retention and access by the state. Its provisions do not require a warrant to be any narrower than a direction under Telecommunications Act 1984 s 94, which was held in *PI* at [80]–[82] to be a regime of general and indiscriminate retention and transmission to the state. Accordingly, Part 6 Chapter 3 is ~~bulk equipment interference warrants are~~ incompatible with EU law on each of the following alternative bases~~because they~~:

(1) Bulk hacking warrants may be issued "in the interests of national security", whether or not on other grounds (ss 178(1)(b), (2)). If and insofar as this purpose is any wider than ~~are not limited to~~ the purpose of ~~fighting serious crime or, alternatively, to~~ preventing the most serious threats to national security (as defined in *PI* and *La Quadrature*), it is incompatible with EU law or, alternatively, it must be construed as so limited to ensure that it is compatible with EU law[181j] (see paragraph 96B above). To the extent to which "the interests of national security" extend beyond these matters, the provisions enable ~~so as to allow~~ the issue of a warrant for purposes that are not capable of justifying an interference with Article 7 and 8 rights (see paragraphs 91–92 and 95–96B above);

~~(2) alternatively, amount to power authorising the indiscriminate and general retention of information and communications obtained and therefore affect the essence of the Article 7 and 8 rights; and/or~~

[181j] See Case C-106/89 Marleasing SA v La Comercial Internacional de Alimentacion SA ECLI:EU:C:1990:395 [9].

(3) In addition, Part 6 Chapter 3 permits the state to **retain and access** information including communications and equipment data (after it has been initially obtained) **other than** for the purpose of preventing the most serious threats to national security. This occurs where an operational purpose (for which information may be selected for examination) is included in a warrant but is not itself referable to "*the interests of national security*", and is instead referable to the serious crime purpose or to the economic purpose: see ss 176(4), 178(1)(d), (2), 183(4), 193(1)(a), (2). To that extent the regime for bulk hacking warrants is incompatible with EU law, as it constitutes a regime of general and indiscriminate retention and access other than for the purpose of preventing the most serious threats to national security. Further, the information obtained is ~~alternatively, are~~ not limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, so do not permit the retention of only that data which is strictly necessary.

(4) Insofar as Part 6 Chapter 3 (read with other provisions of the Act or subordinate legislation) permits CSPs and/or the state to carry out automated processing of data, it does not contain requirements that the model or criteria be specific and reliable, non-discriminatory (including that they are not based on sensitive matters in isolation) and regularly re-examined or that any positive result is individually reviewed before action adversely affecting an individual is taken, as set out in paragraph 102B above.

(b) Non-compliance with further Watson requirements

151. Further or alternatively, insofar as Part 6 Chapter 3 permits information including communications and equipment data to be accessed and/or retained and/or otherwise processed under a bulk equipment interference warrant **other than** for the purpose of preventing the most serious threats to national security (or for operational purposes referable to those other purposes), ~~T~~the power to issue bulk equipment interference warrants fails to comply with the *Watson* requirements in each of the following alternative respects, namely, that it:

~~(1) is not strictly limited to defined and precise offences (nor even to preventing serious crime);~~

~~(2) does not ensure that continued access to data (or its retention) is connected to the objective pursued or depends on a link between continued access/retention and preventing serious crime (alternatively, a serious threat to national security);~~

~~(3) does not, as a general rule, limit government's access to data of individuals suspected of planning, committing, having committed or otherwise been implicated in serious crime (allowing access to the data of other persons only in a specific case and to protect vital national security, defence or public security interests);~~

~~(4) does not require a reasoned application from a national authority to request interception or access;~~

(5) does not require judicial or independent approval each time data is accessed, on the basis of a reasoned application from a national authority to request interception or access (save insofar as a targeted examination warrant is required to access data);

(6) does not require notification of any person affected as soon as that notification is no longer liable to jeopardise investigations being undertaken; and/or

(7) does not require data to be retained in the EU (and section 192 permits data to be provided to "*overseas authorities*" and further allows the disapplication of all retention and disclosure safeguards under Chapter 6 Part 3 in those circumstances).~~;~~

~~(8) does not require providers of electronic communications services to guarantee a particularly high level of protection (as s 191(5) requires only arrangements for storage in a secure manner, rather than a high level of protection);~~

~~(9) does not impose definitive retention periods or impose or require retention periods to be based on objective criteria or adapted depending on the usefulness of material obtained (see s 150(5)–(6)); and/or~~

~~(10) it (and the provisions in Part 8) do not require consideration by an independent authority specifically directed to compliance with the level of data protection required by EU law.~~

(ba) Non-compliance in respect of all purposes with the CFR requirements for sufficient and detailed safeguards equivalent to those under the ECHR

151A. Further or alternatively, Part 6 Chapter 3, in respect of all purposes for which information may be obtained, retained, used and/or otherwise processed, does not comply with the requirements of ECHR Articles 8 and 10 for secret surveillance regimes as set out in paragraphs 139–147 above (and further in the Claimant's Skeleton Argument dated 10 May 2019 before the Divisional Court and the Skeleton Argument of National Union of Journalists dated 10 May 2019). As CFR Articles 7, 8 and 11 provide at least equivalent protection, Part 6 Chapter 3 is also incompatible with those provisions and accordingly incompatible with EU law.

(c) CFR Articles 7 and 11 and journalistic protection / lawyer–client communications

152. Liberty repeats paragraphs 148 and 148 above by reference to CFR Articles 7 and 11.

~~*(d) Article 18 TFEU and Article 21 CFR: Discrimination*~~

~~152A. Liberty repeats paragraphs 149B–149F above by reference to Article 18 TFEU and Article 21 CFR (see also paragraph 106A above).~~

G GROUNDS OF CHALLENGE: THEMATIC HACKING (PART 5)

153. A brief overview of Part 5 is at paragraph 18(4) above. It permits the issue of targeted and thematic equipment interference (hacking) warrants. As mentioned above, Liberty challenges ~~only~~ thematic warrants and targeted warrants insofar as they do not require reasonable suspicion. In broad summary, the Part 5 power:

(1) Authorises or requires the securing of "*interference*" with equipment for the purpose of obtaining "*communications*", "*equipment data*" and "*any other information*" (s 99(2)), although this power cannot be used to intercept communications during transmission that are not stored (s 99(7)–(8)) — it seems that, once communications, equipment data or other information have been "obtained", they may be read, listened to or viewed and otherwise used (although there is no express provision to this effect);

(2) Must relate to any one or more of the following (s 101(1)):

> "(a) equipment belonging to, used by or in the possession of a particular person or organisation;
> (b) equipment belonging to, used by or in the possession of a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
> (c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation;
> (d) equipment in a particular location;
> (e) equipment in more than one location, where the interference is for the purpose of a single investigation or operation;
> (f) equipment which is being, or may be, used for the purposes of a particular activity or activities of a particular description;
> (g) equipment which is being, or may be, used to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, equipment data or other information;
> (h) equipment which is being, or may be, used for the training of persons who carry out, or are likely to carry out, such interference with equipment."

Details of which of these bases a warrant uses, and details of the relevant persons or locations, must be included in the warrant (s 115). As stated, Liberty challenges Part 5 insofar as it confers power to issue the warrants mentioned in s 101(1)(b)–(h) ("**thematic equipment interference warrants**") generally and insofar as it confers power to issue the warrants mentioned in s 101(1)(a) ("**targeted equipment interference warrants**") because reasonable suspicion is not required; and

(3) May be issued by the Secretary of State where considered necessary and proportionate in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom insofar as it these interests are relevant to the interests of national security (s 102(1)(a), (5)). In addition, they may be issued by a law enforcement chief (as set out in Part 1 or 2 of Schedule 6) if necessary and proportionate for the purpose of preventing death or any injury or damage to, or mitigating any injury to, a

person's physical or mental health (s 106(1)), so long as there is a "British Islands connection" (s 107(1)).

(1) Incompatibility with ECHR

(a) Absence of individual targeting and reasonable suspicion

154. The power to issue thematic equipment interference warrants is incompatible with Articles 8 and 10 ECHR because these warrants are not:

(1) limited by reference to an individual/set of premises ~~(or an individual operation or investigation)~~;[182] and/or

(2) alternatively, permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

154A. In addition, the power to issue targeted equipment interference warrants is incompatible with Articles 8 and 10 ECHR because these warrants are not permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

154B. Bulk EI CoP [5.10]–[5.19] makes clear that the Defendants consider (correctly) that the power to issue targeted and thematic equipment interference warrants are not limited in those ways. It makes no reference to any need for suspicion. Further, it indicates (at [5.10]–[5.11]) that no individual need be identified in the warrant and states (at [5.12] that: "*thematic warrants can cover a wide range of activity; it is entirely possible for a thematic warrant to cover a wide geographical area or involve the acquisition of a significant volume of data, provided the strict criteria of the Act are met*". It purports to require (at [5.15]) that descriptions of persons, organisations or locations are "*as granular as reasonably possible*" but states (at [5.16]) that "*it may not always be reasonably practicable to include the names or descriptions of each and every one of the persons, organisations or locations*".

---

[182] ~~Insofar as s 101(1)(c) and (d) appear to confine the warrants they would allow to be issued to one investigation or operation, it is not clear that "investigation" or "operation" have the same meaning as in the ECtHR's case law. For example, in ss 101(1)(c) and (e), equipment in multiple locations is identified by reference to the undefined concept of one "operation" or "investigation" – in this way, "UK anti-terror operations" could be an operation under sections 101(1)(c) and (e).~~

(b) Consideration of critical factors

155. Further or alternatively, the power to issue thematic equipment interference warrants is incompatible with Articles 8 and 10 ECHR because it lacks sufficient safeguards, detail and clarity as to each of the critical features (and, further, the critical features taken together) in the following respects:

156. **Scope of application:** The scope of the thematic hacking provisions is again wide, and in some respects wider than the criteria for bulk powers.

(1) Section 101(1) defines the equipment to which a thematic equipment interference warrant may relate by its connection to particular people, groups of people and activities, which represent the categories of person whose information may be obtained. These connections become very distant and are ill defined. For example:

(a) equipment need only be "*used by*" an individual, organisation, premises or group, but Part 5 does not define the necessary level of use — if use on one occasion suffices, this would permit warrants in very wide circumstances;

(b) equipment may be interfered with where it "*belongs to*" the identified person, even if it is not and has never been in their possession;

(c) equipment can be that which is connected with (belongs to, used by or in the possession of) an altogether indeterminate group with a common purpose or who carries on or even may carry on a particular activity (s 101(1)(b)); and

(d) the category of equipment which is or may be used for the purposes of a particular activity or activities is indeterminate (s 101(1)(f)) — it could, for example, extend to all equipment used for "computing".

(2) Thematic equipment interference warrants are not required to describe, and thereby to limit, the information it is their purpose to retrieve (by contrast even to bulk equipment interference warrants).[183]

(3) No factors for searching the equipment interfered with need be specified in a warrant, ~~by contrast to the thematic carry conditions,~~ so a warrant allows

[183] See ss 99(2), (4) and 115(3), (4) and compare (for bulk equipment interference warrants) s 176(4)(a).

information on any equipment (within the warrant's scope) to be captured and examined.

(4) The range of conduct permitted by the undefined[184] concept of "*interference*" is wide, and wider than the interception of communications considered in past cases such as *Liberty v United Kingdom*.[185] Interference is not limited to intercepting communications during storage or transmission in a public telecommunications system but encompasses potentially altering the data found or a device (s 99(5)(a)); "equipment" is a wider concept than a "*telecommunications system*"; and warrants may authorise the retrieval of any information (save for live interception). For example, a thematic hacking warrant could be used to require the video cameras on all computers or mobile phones used, owned by or that belong to members of a certain group to be activated and transmit their feed to the addressee of the warrant.

(5) The purposes for which thematic equipment warrants may be issued are themselves wider than those for any of the bulk powers and go beyond those of the powers in issue in *Kennedy*:[186] they may be issued for any of national security, preventing and detecting serious crime,[187] the economic well-being of the United Kingdom linked to national security, and preventing death or any injury to physical/mental health or mitigating any injury or damage to a person's mental or physical health (see paragraph 153(3) above).[187a] (The requirement for a ~~limit on the~~ British Islands connection does not reduce the exposure of people in the British Islands to interception for all these purposes.)

---

184 "Interference" is defined in s 48(4) but only for the purpose of authorising OFCOM to intercept certain communications.

185 *Liberty v United Kingdom* (App No 58243/00, 1 July 2008, Fourth Section) [17], [64].

186 *Kennedy v United Kingdom* (App No 26839/05, 18 May 2010, Fourth Section) [159].

187 "Serious crime" is defined widely in s 263(1) as crime where (1) the offence which the conduct would constitute is one for which a person over 21 with no previous convictions could reasonably be expected to receive a sentence of three years or more or (2) the conduct "*involves the use of violence*", results in "*substantial financial gain*" or is "*conduct by a large number of persons in pursuit of a common purpose*".

187a The purported requirement in Bulk EI CoP [4.13] that equipment interference warrants will be issued for the purposes of preventing death or injury or mitigating any injury to a person's physical or mental health only in "*exceptional circumstances*" adds nothing to the certainty of the scope of the power because: it is indeterminate; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(6) A range of people other than the Secretary of State may issue thematic equipment interference warrants, in particular in relation to the last mentioned purpose (ss 103, 106).

(7) Further, Liberty repeats paragraph 110(3) above: a thematic hacking warrant may require or permit thematic hacking, so confers yet further discretion (and room for misuse) on the executive.

157. **Duration:** The duration of thematic equipment interference warrants is six months (or, if issued urgently without Judicial Commissioner approval but later approved, five working days), although they are subject to renewal (ss 116–17). A warrant must be cancelled where the Secretary of State or a senior official (or another person who issued the warrant) considers it no longer necessary or proportionate (s 125). However, there is no statutory duty upon either the Secretary of State or a senior official to keep thematic equipment interference warrants under review.[187b]

158. **Authorisation procedure:**

(1) Liberty repeats paragraph 112 above (save as to modifications to warrants): a Judicial Commissioner approves the warrant and reviews the Secretary of State's (or other decision-maker's) conclusions on necessity/proportionality (ss 102(1)(d), 108(2)(b)), but: (i) the Judicial Commissioner applies only a judicial review standard without reasons for/opposition to the decision (s 108(2));[187c] (ii) an

---

[187b] The purported requirement upon intelligence agencies (not the Secretary of State) to keep warrants under review in Bulk EI CoP [5.30] and [5.101] does not contribute to the certainty of the duration of a warrant because: it does not state who (which person) must do this, with what regularity, by what means or on the basis of what materials; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The similar requirements in Bulk EI CoP [9.19]–[9.20] for equipment interference authorities to undertake "[r]*egular*" reviews of warrants "*as frequently as is considered necessary and proportionate*" suffer from the same vices.

[187c] Further, the purported requirement in Bulk EI CoP [5.2] that there is a review within the agency prior to an application being made does not increase the certainty of the authorisation procedure because: there is no requirement for the reviewer to be independent from the person or team seeking the authorisation; the reviewer is not empowered to prevent an application if they consider that an application is not necessary or proportionate; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements for applications in Bulk EI CoP [4.25], [5.34] and [5.56] do not increase the certainty of the authorisation procedure because: they do not state that an application may not be made if it does not include (a satisfactory) explanation of any of the matters referred to (and do not make any other provision for this circumstance); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61

incomplete warrant may be served on someone to compel assistance in execution, so that person cannot verify authorisation/implementation (s 126(2), (5));[187d] and (iii) combined warrants are permitted but not required (see Schedule 8), so the approvals process may not take into consideration all interference from separate warrants.[187e]

(1A) In addition, thematic equipment interference warrants can be issued in the first instance urgently, that is, without Judicial Commissioner approval for up to three working days (ss 102(1)(d), 104(1)(d), 106(1)(d), 106(3)(d), 109(3)). Non-approval after the fact by the Judicial Commissioner does not affect the lawfulness of anything done before the Judicial Commissioner's decision (s 110(9)), there is no definition in the Act of "urgency"[187f] nor any review of the decision to approve urgently (s 180),[187g] and non-approval by the Judicial Commissioner enlivens only a discretion of the Judicial Commissioner, rather than any requirement, to destroy or impose conditions on the use of the underlying material (s 110(3)).

(2) In general, modifications to a warrant — including to expand the equipment to which it relates — do not require Judicial Commissioner approval (except where

---

above). The purported requirement that a Judicial Commissioner has access to the same application as the Secretary of State (or other decision-maker) in Bulk EI CoP [5.61] also does not increase the certainty of the authorisation procedure because: there is no provision that a Judicial Commissioner may not approve a warrant if this is not the case; and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[187d] Bulk EI CoP [7.15]–[7.16] confirms that telecommunications operators will not be given entire warrants, in that it states part only of a warrant may be given to a telecommunications operator and states that a telecommunications operator "*will not necessarily be provided with all the information contained in the warrant*". This makes it hard or impossible for a telecommunications operator or other person to exercise supervision over whether retention and acquisition are in accordance with a warrant.

[187e] Bulk EI CoP [5.105] confirms that: "*Combining warrant applications is not mandatory.*" It further states that combined warrants allow "*a more informed decision about the necessity and proportionality of the totality of the action being undertaken*".

[187f] This ambiguity is made worse by the Bulk EI CoP containing at least two differing definitions of "urgency", which themselves are confusing. Bulk EI CoP [5.67] and [6.29] state that urgency is determined by "*whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the time available to meet an operational or investigative need*" (which is vague and indeterminate), but go on to say that an urgent situation "*should fall into one or both*" of two categories, namely, "*imminent threat to life or serious harm*" and "*an intelligence-gathering or investigative opportunity with limited time to act*" (again an indeterminate category). Bulk EI CoP [5.91] states that a modification "*will only be considered urgent if there is a very limited window of opportunity to act*", suggesting a different (and wider) test. In any case, these definitions are not a statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[187g] On the absence of any review of whether it was appropriate to approve a warrant urgently, see above n 181.

they are urgent): ss 118–22. Instead, a Judicial Commissioner is notified of the modification, but lacks power to refuse it (s 121). Further, there is no definition of when it is "urgent" to make a modification, so that this concept, and thus the trigger for Judicial Commissioner approval, remains in the discretion of officials (ss 119(2), 122).

159. **Procedure for use/examination/storage and precautions when communicating:** Sections 129 and 130~~109~~ require "*arrangements*" that create some safeguards for use, examination, secure storage and precautions when communicating communications or other information obtained. These safeguards can be disapplied altogether where the material obtained is given to overseas authorities (s 130(2)). The safeguards may also be disapplied where communications that are intercepted are retained under Part 7 (s 225(4)–(6)).[187h] ~~In any case, so far as Liberty is aware, there are no such arrangements in force.~~

160. **Circumstances of destruction:** Section 129(5) requires an arrangement to be in force that "*every copy made of any … material*" is destroyed once there are no longer grounds for retaining it. However, under s 129(5)–(7~~6~~), obtained material can be retained (i) where it is "*necessary*" or "*likely to become necessary*" and (ii) this may be on the basis of any ground on which a warrant could have been issued (not the ground on which it was issued). In addition, even if arrangements exist under s 129(5) for the destruction of "*every copy made of any of that material*" once there are no longer grounds under s 129(6) for retaining it:

    (1) This appears to require only that "copies", and not the "material" itself (that is, the original hacked material), are destroyed, given the definition of "copy" in s 129(9) and the distinction s 129 draws between the "material" and a "copy" of it;

[187h] The purported requirements in Bulk EI CoP [9.22], [9.30] and [9.31] in relation to dissemination, copying, storage and destruction of material obtained under interception warrants do not materially add to the statutory provisions themselves because they are: vague, general and subjective (for example, [9.31] states that retention periods "*should normally be no longer than two years*"); and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Further, the purported requirements in Bulk EI CoP [9.22] and [9.28] that retained data should be held such that only security-cleared and trained persons should be able to access it and authorised persons are granted access only where it is necessary for them to have access do not increase the certainty of the access procedure because: they are vague and general and, in consequence, do not impose any real limits on what may occur; and in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(2) In any event, the nature of the wider categories of thematic interception means that irrelevant data will inevitably be interceptedbe destroyed only if and when it is examined. There is no statutory limit on the retention of obtained material., and it is possible to know whether there are grounds for retaining the obtained material under s 150(6) only by examining it. In consequence, thematic hacking warrants are likely also to result in "*the automatic storage of clearly irrelevant data*", which the Grand Chamber in *Zakharov* held "*cannot be considered justified under Article 8*";[188] and

(3) Further, these safeguards may be disapplied where communications that are intercepted are retained under Part 7 (s 225(4)–(6)) or provided to any overseas authorities (ss 129(9)–(10), 130(2)).

161. **Notification and remedies:** Liberty repeats paragraph 146 above.Notification is very rarely required under the Act and, where required, in the IPCr's discretion, and the ability to apply to the IPT for investigation is a far weaker safeguard than previously thought (see paragraphs 115–116 above).

162. For the foregoing reasons, the power to issue thematic equipment interference (hacking) warrants under Part 5 is not "in accordance with the law" or "provided by law" and/or not "necessary in a democratic society" under Articles 8 and 10 ECHR.

(c) ECHR Articles 8 and 10 and journalistic protections

163. Sections 113 and 114 provide that, where an applicanttion for a warrant under Part 5 believes that the information obtained under the warrant will be communications or other items containing "*confidential journalistic material*" (s 113(1)(a)) or where the purpose of the application is to identify or confirm a "*source of journalistic information*" (as defined in s 263) (s 114(1)), the application must contain a statement to either effect and the person to whom the application is made may not issue the warrant unless they consider that the s 129 arrangements include specific arrangements for the handling, retention, use and destruction of communications or other items of information containing confidential journalistic material or identifying sources of journalistic information.

---

188 *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [255].

164. ~~No such arrangements are, as far as Liberty is aware, currently in force. Further, e~~Even if the arrangements described (for the handling, retention, use and destruction of the confidential journalistic information or material identifying a journalistic source) exist, this would not satisfy one of the mandatory requirements under ECHR Article 10. There is no requirement that ~~that~~ (see paragraph 67 above) the Secretary of State deciding or the Judicial Commissioner in approving the application has regard to the need for an overwhelming public interest to justify the revealing of a journalistic source.[188a]

165. Part 5 is accordingly incompatible also with ECHR Article 10.

(d) ECHR Articles 8 and 10 and lawyer–client communications

166. Sections 112 and 131 make some provision for protection of items subject to legal privilege. However, these protections are inadequate to comply with the requirements under Articles 8 and 10 ECHR (as set out in paragraph 71 above) in that they:

(1) do not apply to all lawyer–client communications but, instead, only to those items that are actually "*subject to legal privilege*" (ss 112(1), (7), 131(1)) or which would be but are made or created with the intention of furthering a criminal purpose (s 112(11));

(2) do not provide for who is to determine whether communications are (or are likely to be) legally privileged or for that person to be independent:

(a) there is no express requirement for an independent person to determine whether the items are or are likely to be privileged or are not privileged because they were made to further a criminal purpose;[189]

[188a] Bulk EI CoP [9.76] purports to require that, where an equipment interference warrant is sought "*to determine the source of journalistic information*", then "*the public interest requiring such selection must override any other public interest*". However, this does not apply outside situation where a warrant is sought to reveal the source (including, for example, where it is likely that a journalistic source will be revealed (see Bulk EI CoP [9.74]) or where a journalist's information is obtained); and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[189] Although, in the last case, the person to whom the application is made may issue the warrant only if they consider it likely that the communications were made or other information was created with the intention of furthering a criminal purpose: s 112(13).

(b) the applicant (who is not independent)[190] will have to have considered this to mention it in the application for a targeted equipment interference warrant (as required under ss 112(2), (8) and (12)), as will the addressee of a warrant (who is not independent) who alerts the IPCr that privileged material has been retained (under s 131(1)–(2));

(c) none of the Secretary of State, the Scottish Ministers or a law enforcement chief, who issue targeted equipment interference warrants and must reach the conclusions in relation to privileged material required by ss 112(4), (9) and (13), is independent (and Judicial Commissioners lack power under s 108(1) to review their conclusions under those provisions);

(3) do not require an assessment of whether a communication or information is subject to strengthened protection under Articles 8 and 10 in all circumstances before it is intercepted, obtained or used (instead, s 112(1), (7) and (11) require special approval of targeted equipment interference warrants only where a purpose is to obtain legally privileged items, material obtained is likely to included legally privileged items, or a purpose is to obtain items that would be legally privileged if they had not been created with the intention of furthering a criminal purpose — where privileged items are otherwise obtained (for example, unexpectedly or where this was not likely), s 131(2) requires that the IPCr be informed as soon as is reasonably practicable but does not prevent any use of the item until the IPCr decides whether it should be destroyed or conditions should attach to its use under s 131(3)–(7)); and/or

(4) fail to ensure proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations except where a purpose of the warrant is to obtain items subject to legal privilege (only in this situation does s 112(1)–(6) require the person to whom the application is made to have regard to "*the public interest in the confidentiality of items subject to legal privilege*" or whether there are "*exceptional and compelling circumstances that make it*

[190] Who is (someone acting on behalf of) the head of an intelligence service (ss 102(1), 103(1)), the Chief of Defence Intelligence (s 104(1)), and an appropriate law enforcement officer in relation to a law enforcement chief (s 106(1), (5)), and therefore not independent.

necessary to authorise the interference with equipment": see s 112(1), (3), (4)(a) and compare s 112(7)–(9) and (11)–(13)).

166A. The Bulk EI CoP[190a] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are required,[190b] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[190c]

(2) Incompatibility with EU law

(a) General and indiscriminate retention of content of communications

167. Liberty repeats paragraph 120 above: thematic equipment interference warrants are incompatible with EU law because, at least in respect of warrants issued under s 101(1)(b), (c), (e) and (f), the breadth and the absence of **requirements** to limit the scope of a warrant in Part 5 mean it constitutes a general and indiscriminate regime of retention and access by the state. In those circumstances it is incompatible with EU law on each of the following alternative bases:

(1) Thematic hacking warrants may be issued "in the interests of national security" (ss 102(5)(a), 104(1)(a)). If and insofar as this purpose is any wider than preventing the most serious threats to national security (as defined in *PI* and *La Quadrature*), it is incompatible with EU law or, alternatively, it must be construed as so limited

---

[190a] Bulk EI CoP [9.44]–[9.54], [9.58]–[9.69].

[190b] In particular, the Bulk EI CoP does not: (1) provide for who is to determine whether communications are (likely to be) lawyer–client communications or require this to be determined by an independent person (but, in relation to targeted and thematic warrants, provides only for consultation of a legal adviser within the equipment interference authority where there is doubt about privilege: Bulk EI CoP [9.46]); (2) require an assessment of whether a lawyer–client communication is subject to strengthened protection under Articles 8 and 10 ECHR in all circumstances before it is obtained, selected for examination or further used (instead, only where privileged communications are likely to be obtained or it is the purpose of the warrant to obtain them, and not before any further use: see Bulk EI CoP [9.49]–[9.51]); (3) require proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations where they are obtained, selected for examination or used (save where it is the purpose of selection for examination to obtain privileged communications, in which case the issuing authority must be satisfied that there are "*exceptional and compelling circumstances*" that make the warrant necessary: Bulk EI CoP [9.50]).

[190c] This applies in particular to the purported requirement in Bulk EI CoP [9.58]–[9.60] to assume that s 194 applies where a lawyer acting a professional capacity is the subject of a targeted examination warrant or subject of examination.

to ensure that it is compatible with EU law[190d] (see paragraph 96B above). To the extent to which "the interests of national security" extend beyond these matters, the provisions enable the issue of warrants incapable of justification as strictly necessary (see paragraphs 91–92 and 95–96B above).

(2) In addition, thematic hacking warrants may be issued to permit the state to obtain, retain and access information for purposes other than preventing the most serious threats to national security, namely, ~~they are not limited to the purpose of fighting serious crime or, alternatively, to serious threats to national security, preventing and detecting~~ the serious crime purpose, ~~and to serious concerns about~~ the economic purpose ~~well-being of the United Kingdom insofar as it concerns national security~~, and preventing death or injury or damage to a person's physical or mental health or mitigating any such damage (ss 102(5)(b)–(c), 106(1), 106(3)). To that extent the regime for thematic hacking is incompatible with EU law, as it constitutes a regime of general and indiscriminate retention and access other than for the purpose of preventing the most serious threats to national security. It ~~so as to~~ allows the issue of a warrant for purposes that are not capable of justifying ~~an~~ such a serious interference with Article 7 and 8 rights.

(3) Insofar as Part 5 (read with other provisions of the Act or subordinate legislation) permits CSPs and/or the state to carry out automated processing of data, it does not contain requirements that the model or criteria be specific and reliable, non-discriminatory (including that they are not based on sensitive matters in isolation) and regularly re-examined or that any positive result is individually reviewed before action adversely affecting an individual is taken, as set out in paragraph 102B above.

(b) Non-compliance with further Watson requirements

168. Further or alternatively, insofar as Part 5 permits content and/or secondary data to be obtained, accessed, retained and/or otherwise processed under a thematic hacking warrant **other than** for the purpose of preventing the most serious threats to national security, ~~T~~the power to issue thematic equipment interference warrants, at least in respect

[190d] See Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* ECLI:EU:C:1990:395 [9].

of warrants issued under s 101(1)(b), (c), (e) and (f), fails to comply with the *Watson* requirements in each of the following alternative respects, namely, that it:

~~(1) is not strictly limited to defined and precise offences (nor even to preventing serious crime);~~

~~(2) does not ensure that continued access to data (or its retention) is connected to the objective pursued or depends on a link between continued access/retention and preventing serious crime (alternatively, a serious threat to national security);~~

~~(3) does not, as a general rule, limit government's access to data of individuals suspected of planning, committing, having committed or otherwise been implicated in serious crime (allowing access to the data of other persons only in a specific case and to protect vital national security, defence or public security interests);~~

~~(4) does not require a reasoned application from a national authority to request interception or access (save for the specific requirements in ss 113 and 114 in relation to journalistic information and sources, which are insufficient requirements for this purpose);~~

(5) does not require judicial or independent approval each time data is accessed, on the basis of a reasoned application from a national authority to request interception or access (save for the specific requirements in ss 113 and 114 in relation to journalistic information and sources, which are insufficient requirements for this purpose);

(6) does not require notification of any person affected as soon as that notification is no longer liable to jeopardise investigations being undertaken; and/or

(7) does not require data to be retained in the EU (and section 192 permits data to be provided to "*overseas authorities*" and further allows the disapplication of all retention and disclosure safeguards under Chapter 6 Part 3 in those circumstances).~~;~~

~~(8) does not require providers of electronic communications services to guarantee a particularly high level of protection (as s 129(4) requires only arrangements for storage in a secure manner, rather than a high level of protection);~~

~~(9) does not impose definitive retention periods or impose or require retention periods to be based on objective criteria or adapted depending on the usefulness of material obtained (see s 29(5)–(6)); and/or~~

~~(10) it (and the provisions in Part 8) do not require consideration by an independent authority specifically directed to compliance with the level of data protection required by EU law.~~

(ba) Non-compliance in respect of all purposes with the CFR requirements for sufficient and detailed safeguards equivalent to those under the ECHR

168A. Further or alternatively, Part 5, in respect of all purposes for which data may be obtained, retained, used and/or otherwise processed, at least in respect of warrants issued under s 101(1)(b), (c), (e) and (f), does not comply with the requirements of ECHR Articles 8 and 10 for secret surveillance regimes as set out in paragraphs 154–162 above (and further in the Claimant's Skeleton Argument dated 10 May 2019 before the Divisional Court and the Skeleton Argument of National Union of Journalists dated 10 May 2019). As CFR Articles 7, 8 and 11 provide at least equivalent protection, Part 5 is also to at least that extent incompatible with those provisions and accordingly incompatible with EU law.

(c) CFR Article 11 and journalistic protection / lawyer–client communications

169. Liberty repeats paragraphs 164 and 166 above by reference to CFR Articles 7 and 11.

H GROUNDS OF CHALLENGE: GENERAL RETENTION AND ACCESS (PARTS 3 AND 4)

170. A brief overview of Part 4 (and Part 3) is at paragraph 18(5) above. Part 4 permits the imposition of a general and indiscriminate obligation to retain data. In broad summary, the Part 4 power to issue a "**retention notice**":

(1) Requires by s 87(1) a telecommunications operator to retain "*relevant communications data*".[191] This may include all communications data and as yet non-existent communications data (s 87(2)). Retention may be for at most 12 months from specified dates (s 87(3));[192]

(2) ~~Requires~~As enacted, required the Secretary of State to consider that the requirement is necessary and proportionate (s 87(1)) for ~~our~~one or more of the purposes in s 61(7)(a)–(j):

> "(a) in the interests of national security,
> (b) for the purpose of preventing or detecting crime or of preventing disorder,
> (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
> (d) in the interests of public safety,
> (e) for the purpose of protecting public health,
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
> (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
> (h) to assist investigations into alleged miscarriages of justice,
> (i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition —
> (i) to assist in identifying P, or
> (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or
> (j) for the purpose of exercising functions relating to —
> (i) the regulation of financial services and markets, or
> (ii) financial stability."

---

191 That is, communications data which may be used to identify the sender/recipient of a communication, its time/duration, the type/method/pattern or the fact of communication, the telecommunications system used for the communication or the location of that system, including internet connection records: s 87(11).

192 It is unclear whether the effect of ss 87(3) and (5) is that a telecommunications operator is obliged to retain data that exists when a Part 4 retention notice is issued for 12 months from the issue of the notice or only for 12 months from the telecommunications operator's initial receipt of the data (regardless of when the notice is issued). If the former construction is correct, the duration of retention could be extended indefinitely by issuing new retention notices just before 12 months expire.

However, in consequence of this claim (amongst other matters) and in light of the Defendants' concessions set out above, the draft Data Retention and Acquisition Regulations 2018 **[CB/2B/2(g)/445.001]** ~~have been~~ were laid before Parliament on 28 June 2018. They came into force on 1 November 2018. ~~It is easiest to understand the proposed amendments from the Keeling Schedule containing them which appears also to have been laid before Parliament [CB/2B/2(h)/445.029]. If made, t~~These regulations ~~would~~ limit the purposes for which a retention notice may be given and data retained under it may be accessed by the state to the following (which are ~~to be~~ set out in a new s 87(1)(a)):

> "(i) in the interests of national security,
> (ii) for the applicable crime purpose (see subsection (10A)),
> (iii) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
> (iv) in the interests of public safety,
> (v) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
> (vi) to assist investigations into alleged miscarriages of justice"

For this purpose, a new s 87(10A) ~~will~~ defines "*the applicable crime purpose*" as follows:

> "(a) to the extent that a retention notice relates to events data, the purpose of preventing or detecting serious crime;
>
> (b) to the extent that a retention notice relates to entity data, the purpose of preventing or detecting crime or of preventing disorder."[192a]

Additionally, a new s 87(10B) provides that, for the purposes of s 87(10A)(a), "serious crime" means:

[192a] ~~Further, a new s 87(10B) will define "serious crime" as crimes which fall within paragraphs (a) and (b) of the definition of that term in s 263(1) and add to that definition: (i) offences for which an 18 year old individual is capable of being sentenced to imprisonment for a term of 12 months or more; and (ii) offences by persons who are not individuals or which involve, as an integral part, the sending of a communication or a breach of a person's privacy.~~

(a) those crimes within the definition in s 263(1), that is, crime where: (i) the offence(s) that would be constituted by the conduct concerned is an offence for which a person over the age of 18 with no previous convictions could reasonably be expected to be sentenced to imprisonment for three years or more or (ii) the conduct involves the use of violence, results in substantial financial gain, or is conduct by a large number of persons in pursuit of a common purpose; and

(b) in addition, crime where the offence(s) that would be constituted by the conduct concerned is:

(i) any offence with a penalty of 12 months' imprisonment or more (s 87(10B)(a));

(ii) an offence by a person who is not an individual (s 87(10B)(b)(i)), which includes any offence by a body corporate;

(iii) an offence that involves as an integral part the sending of a communication or a breach of a person's privacy (s 87(10B)(b)(ii)).

(3) Part 3 is one means by which the state can access the data retained under Part 4. It provides, following amendment, as follows:

(a) ~~for designated senior officers in~~ For local authorities and other relevant public authorities ("**RPAs**") (~~local authorities and those listed in Schedule 4:~~ see ss 71, 73), the IPCr, in practice, the Investigatory Powers Commissioner's Office ("**IPCO**"), may ~~to~~ authorise the RPA to engage in conduct to obtain communications data under s 60A. ~~They~~The IPCr may do so on the application of such an RPA where this is necessary and proportionate for a ~~s 61(7)~~ purpose in s 60A(7) (s 60A(1)(a), (c)) and where it is necessary for the purposes of a specific investigation/operation (or for testing equipment systems) (s ~~61(1)~~60A(1)(b)). The purposes in s 60A(7) are those in s 87(1)(a) with one addition, namely, the purpose of assisting in identifying a person or obtaining information about their next of kin, other persons connected with a person or the reason for their death or condition where a person has died or is unable to identify themselves because of a physical or mental condition.

For local authorities and RPAs listed in the table Schedule 4 without any authorisation for the purposes of s 61(7) in the fifth column, this is the only means by which they can obtain communications data (save, in respect of certain RPAs listed in Schedule 4 but not local authorities, in urgent circumstances under s 61A). ~~(The proposed amendments to the Act would limit these purposes and would have the effect that non-urgent authorisations other than for national security, preventing/detecting crime and the UK's economic wellbeing as relevant to national security must be authorised by the Investigatory Powers Commissioner: see the proposed ss 60A, 61 and 61A.)~~

(b) In addition, RPAs listed in Schedule 4 with an authorisation for the purposes of s 61(7) in the fifth column, which include certain police forces, the Security Service, GCHQ and the Secret Intelligence Service (and do not include local authorities), may under s 61 **themselves** obtain communications data, with no prior independent authorisation. They may do so where a designated senior office of the RPA (as defined in ss 70–73) considers that it is necessary and proportionate for a purpose in s 61(7) (s 61(1)(a), (c)) and that it is necessary for the purposes of a specific investigation/operation (or for testing equipment systems) (s 61(1)(b)). The purposes in s 61(7) are (a) national security, (b) the "applicable crime purpose" (defined as in s 87(10A) set out above) and (c) the economic purpose.

(c) Further, RPAs listed in Schedule 4 with an authorisation for the purposes of s 61A(7) in the sixth column, which include certain police forces (and do not include the Security Service, GCHQ and the Secret Intelligence Service or local authorities), may under s 61A themselves obtain communications data, with no prior independent authorisation, where a designated senior officer considers that "there is an urgent need to obtain the data": s 61A(1)(c). In addition, the designated senior officer must consider that it is necessary and proportionate for a purpose in s 61A(7) (s 61A(1)(a), (d)) and that it is necessary for the purposes of a specific investigation/operation (or for testing equipment systems) (s 61A(1)(b)). The purposes in s 61A(7) are (a) the "applicable crime purpose" (defined as in s 87(10A) set out above), (b) the

interests of public safety, (c) preventing death or injury or any damage to a person's physical or mental health or mitigating such damage, (d) to assist investigations into miscarriages of justice and assisting in identifying a person or obtaining information about their next of kin, other persons connected with a person or the reason for their death or condition where a person has died or is unable to identify themselves because of a physical or mental condition.

An authorisation under Part 3 permits an officer from an RPA to engage in conduct for the purposes of obtaining the data from any person, directly or from a telecommunications operator (ss 60A(2), (4), 61(2), (4)). Section 66 expressly provides for telecommunications operators' duties to comply with requests. As mentioned above, communications data retained under Part 4 could in addition be the subject of a bulk acquisition warrant under Part 6 Chapter 2.

~~170A. The Defendants have not (so far as Liberty is aware) said publicly if and when the amendments mentioned will commence. Further, the draft regulations were (Liberty understands) laid before Parliament on 28 June 2018. Accordingly, if and to the extent the Act is amended in accordance with those proposed amendments or otherwise, Liberty reserves the right further to plead its case to address any amendments.~~

(1) Incompatibility with EU law

(a) General and indiscriminate retention of ~~content of~~ communications data

171. Liberty repeats paragraph 120 above: the Parts 3–4 regime as amended due to its breadth and the absence of provisions that **require** limitations on the scope of retention notices, remains a regime of general and indiscriminate retention (by CSPs) and access (by the state). ~~regime in Part 4, without and with the proposed amendments,~~ It is incompatible with EU law because ~~it~~:

(A1) Retention notices may be issued "in the interests of national security" (s 87(1)(a)). If and insofar as this purpose is any wider than preventing the most serious threats to national security (as defined in *PI* and *La Quadrature*), it is incompatible with

EU law or, alternatively, it must be construed as so limited to ensure that it is compatible with EU law[192b] (see paragraph 96B above).

(1) Insofar as retention notices may be issued and retained data accessed for purposes other than preventing the most serious threats to national security, namely, ~~is not limited to the purpose of fighting~~ preventing and detecting serious or other crime and ~~or, alternatively, to serious threats to all of the interests~~ the other purposes listed in ss 60A(7), 61(7) and ~~incorporated by s~~ 87(1) ~~or proposed to be included in s 87(1)~~ (set out in paragraph 170 ~~170(2)~~ above) the retention and acquisition regime, as a general and indiscriminate regime, is incompatible with EU law.~~,~~ ~~so in consequence it allows the issue of a warrant~~ It authorises retention of and access to data for purposes that are not capable of justifying such a~~n~~ serious interference with Article 7 and 8 rights.~~; and/or~~ Further, it is not limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, so it fails to permit the retention of only that data which is strictly necessary.

~~(2) alternatively, permits the authorisation of the indiscriminate and general retention of communications data, and is not limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, so it fails to permit the retention of only that data which is strictly necessary.~~

(3) Insofar as Parts 3–4 (read with other provisions of the Act or subordinate legislation) permit CSPs and/or the state to carry out automated processing of data, they do not contain requirements that the model or criteria be specific and reliable, non-discriminatory (including that they are not based on sensitive matters in isolation) and regularly re-examined or that any positive result is individually reviewed before action adversely affecting an individual is taken, as set out in paragraph 102B above.

[192b] See Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion* SA ECLI:EU:C:1990:395 [9].

172. As explained in paragraphs 81–82 above, *Watson* considered the DRIPA retention regime and the RIPA s 22 access provisions which ~~are~~ were substantively identical to Parts 4 and 3 of the Act respectively (prior to the ~~proposed~~ amendments). The CJEU held expressly that they were within the material scope of EU law[193] and, further, that the Swedish legislation in issue imposed an impermissible requirement of "*general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication*".[194] There is for these purposes no difference in principle between the Swedish legislation, which directly imposed a data retention obligation, and DRIPA or Part 4 of the Act (with ~~or without~~ the ~~proposed~~ amendments), which permit an obligation to be imposed (substantially) to the same extent. The CJEU's concern was the State's ability to require telecommunications operators to retain data indiscriminately.[195] Further, CD CoP [19.53] implicitly accepts that Part 4 is within the scope of EU law.[195a]

173. In addition, the Divisional Court in *Watson*, referring to the Defendants' failure to disclose any retention notice under DRIPA, said:[196]

> "the consequence of this policy stance is that we should test the validity of DRIPA on the assumption that the retention notices issued under it may be as broad in scope as the statute permits, namely a direction to each CSP to retain all communications data for a period of 12 months."

The same approach applies here. It follows that the Part 4 power to require the retention of communications data — which by s 87(2)(b) extends to a power to "*require the retention of all data*" of a telecommunications operator and which by s 95(1) the telecommunications operator has a duty to obey — along with the Part 3 access provisions is incompatible with EU law.

---

193 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [81].

194 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [97].

195 See Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* ECLI:EU:C:2016:970 [97]–[99].

195a CB CoP [19.51]–[19.52] purport to require retained communications data to be held within the EU (subject to certain exceptions), and [19.53] says relevantly: "*Once the United Kingdom is no longer a member of the European Union these requirements will not apply as they do while the United Kingdom is a member.*"

196 *R (Davis and Watson) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin), [2016] 1 CMLR 13 [65] (Bean LJ)

(b) Non-compliance with further Watson requirements

174. Further or alternatively, insofar as Parts 3 and 4 permit communications data to be retained, accessed and/or otherwise processed **other than** for the purpose of preventing the most serious threats to national security, ~~T~~the power to issue retention notices under Part 4 (read with the accompanying access provisions in Part 3), ~~without or~~ with the ~~proposed~~ amendments, fails to comply with the *Watson* requirements in each of the following alternative respects (each of which makes it incompatible with EU law), namely, that the power:

~~(1) is not strictly limited to defined and precise offences (nor even to preventing serious crime);~~

~~(2) does not ensure that continued retention of data (or continued access to it) is connected to the objective pursued or depends on a link between continued access/retention and preventing serious crime (alternatively, a serious threat to the interests listed in s 61(7) of the Act);~~

(3) does not require prior independent authorisation of access to data that has been retained on the basis of a reasoned application from a national authority, save insofar as an RPA may request data **only** under s 60A (as to the urgency procedure in s 61A see paragraph 177A(3)(c) below) ~~to request interception or access (instead, under s 87, the Secretary of State decides to issue a notice and a Judicial Commissioner under s 89 approves it)~~. In particular, prior independent authorisation is not required (i) where the Security Service, the Secret Intelligence Service, GCHQ and the Environment Agency access communications data (alternatively events data) under the self-authorisation provision in s 61 for the purpose of preventing and detecting serious crime (for events data) or preventing and detecting crime or preventing disorder (for entity data) nor (i) where the Security Service, the Secret Intelligence Service, GCHQ and the police forces authorised in Schedule 4 access communications data for the economic purpose under s 61. See further paragraph 177A(3)(b) below;

(4) does not require notification of any person affected, ~~(~~that is, ~~whose data has been retained) as soon as that notification is no longer liable to jeopardise investigations being undertaken (nor does~~ Part 3 does not require ~~such~~ notification where access

has occurred but notification is possible — instead, the Act requires only limited provision for after-the-event notification by the IPCr in the case of "*relevant*" and "*serious*" errors and where notification is in the public interest, as set out in paragraph 115 above~~)~~; and

(5) does not require data to be retained in the EU. ~~(and section 192 permits data to be provided to "overseas authorities" and further allows the disapplication of all retention and disclosure safeguards under Chapter 6 Part 3 in those circumstances);~~

~~(6) does not appear to require that providers of electronic communications services to guarantee a particularly high level of protection (as ss 92–93 themselves set out vague, high-level guidelines, rather than a high level of protection);~~

~~(7) does not impose or require retention periods to be based on objective criteria or adapted depending on the usefulness of material obtained (albeit imposing a 12-month retention period by ss 87(4)–(5)); and/or~~

~~(8) it (and the provisions in Part 8) do not require consideration by an independent authority specifically directed to compliance with the level of data protection required by EU law.~~

175. ~~Liberty notes for completeness that the access power in Part 3, without or with the proposed amendments:~~

~~(1) does not, as a general rule, limit government's access to data of individuals suspected of planning, committing, having committed or otherwise been implicated in serious crime (allowing access to the data of other persons only in a specific case and to protect vital national security, defence or public security interests); and~~

~~(2) without the proposed amendments, does not require judicial or independent approval each time data is accessed (the provisions in relation to single points of contact do not provide for this, but merely for advice and contract (see s 76), and the DSO is not independent of the body seeking the warrant: s 63 — it does not suffice that they are, usually, independent of the investigation or operation for which the data is sought).~~

176. In addition, the bulk acquisition regime under Part 6 Chapter 2 does not comply with the *Watson* requirements in many respects, as set out in paragraphs 135–136 above.

177. These additional matters are relevant when considering whether Part 4 of the IPA complies with the *Watson* requirements.

177A. As set out in paragraph 29V above, the Divisional Court accepted some but not all of the incompatibilities with EU law pleaded above and stayed the determination of Part 4 EU Law Claim pending the CJEU's decision in the IPT's Reference in relation to: (1) the application of EU law in the national security context; (2) any requirement under EU law to retain data within the EU; and (3) any requirement under EU law to notify persons after data relating to them has been accessed or used. The order further provides that, upon the decision in the IPT's Reference, the parties shall use their best endeavours to agree order disposing of the stayed part of the claim or directions. Upon the CJEU's decision in the IPT's Reference (if the parties cannot agree appropriate orders), whether or not Parts 3 and 4 have been amended (as proposed or otherwise):

(1) The Court should consider the compatibility with EU law of the Act and the ~~(draft)~~ regulations. ~~As to the latter, if the regulations have not by that time been made, it is nonetheless well-established that draft affirmative regulations (such as those proposed here) laid before Parliament are subject to judicial review: R v Her Majesty's Treasury, ex parte Smedley [1985] QB 657 (CA) 666–667 (Sir John Donaldson MR), 672 (Slade LJ): "where some administrative order or regulation is required by statute to be approved by resolution of both Houses of Parliament, the court can in an appropriate case intervene by way of judicial review before the Houses have given their approval".~~

(2) The draft regulations purport to be made under s 2(2) of the European Communities Act 1972. Accordingly, ~~if the draft regulations are made,~~ to the extent they purport to introduce amendments to the Act that are incompatible with EU law, they are ultra vires, void and of no effect (see *Oakley Inc v Animal Ltd* [2005] EWCA Civ 1191, [2006] Ch 337 [20]–[21], [28]–[29], [39] (Waller LJ), [65], [70], [80] (Jacob LJ)) and, for the reasons above, Part 4 without amendments is incompatible with EU law (and to that extent of no effect).

(3) ~~If regulations in the form of the draft regulations are made then, they are~~ The Act as amended by the regulations is incompatible with EU law (and therefore the regulations are ultra vires, void and of no effect and Part 4 falls to be disapplied) for the reasons set out in paragraphs 171–177 above. Without limitation to and by way of amplification:

(a) ~~Proposed ss~~Sections 60A, 61 and 61A (which provide for access) and s 87 (which provides for retention) do not limit retention and acquisition of communications data (alternatively events data) for the "*applicable crime purpose*" (see the proposed ss 60A(7)(b), (8), 61(7)(b), (7A), 61A(7)(a), (8), 86(2A), 87(1)(a), (10A)–(10B)) to "*the objective of fighting serious crime*" within the meaning of *Watson* (see paragraph 91 above). In particular, while events data may be acquired only for the purpose of preventing or detecting "*serious crime*", ~~proposed~~ s 86(2A) defines "*serious crime*" (as explained in paragraph 170(2)–(3) above) so widely as to make this requirement nugatory:

(i) "*Serious crime*" is defined to include **any** crime by a body corporate (or committed otherwise than by an individual) (~~proposed~~ ss 86(2A)(b)(i) and 87(10B)(b)(i)) and **any** offence which involves "*as an integral part*" the sending of a communication or a breach of privacy (~~proposed~~ ss 86(2A)(b)(ii) and 87(10B)(b)(ii)). However, whether an offence is committed by a body corporate, or involves a communication or breach of privacy, bears no relation to its seriousness.

(ii) "*Serious crime*" is also defined to include any offence that carries a penalty of 12 months imprisonment or more for offenders of 18 years or more (~~proposed~~ ss 86(2A)(a) and 87(10B)(a)). This definition encompasses the vast majority of criminal offences and applies regardless of the particular circumstances of the offence. Narrower definitions are practicable: s 263(1) defines "serious crime" by reference to the particular circumstances, or nature or effects, of the criminal conduct and, insofar as it turns on sentence, applies only where a person without prior convictions could reasonably expect to receive a sentence of three years or more.

(b) ~~Proposed s~~Section 61 does not comply with the *Watson* requirement for prior independent authorisation of acquisition of retained communications data (alternatively events data). It permits authorisation of acquisition of communications data other than by an independent judge or executive body (instead by the acquiring body itself):

(i) for the "*applicable crime purpose*" under ~~proposed~~ s 61(7)(b), by GCHQ, the Secret Intelligence Service and the Security Service and the Environment Agency (see ~~proposed~~ s 70(5A) and the corresponding entries in columns 4–5 of ~~Part 1 of~~ the Table in ~~the proposed~~ Schedule 4); and

(ii) ~~in the interests of national security and~~ in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security under ~~proposed~~ s ~~61(7)(a) and~~ 61(7)(c), by GCHQ, the Secret Intelligence Service and the Security Service and, in addition, various police forces (see ~~proposed~~ s 70(5A) and the corresponding entries in columns 4–5 of Part 1 of the Table in the proposed Schedule 4).

It is apparent from *PI* and *La Quadrature* that ~~If (1)~~ the activities of GCHQ, the Secret Intelligence Service and the Security Service ~~and (2) actions~~even if carried out in the interests of national security and in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security fall within the scope of EU law, ~~as Liberty explains to be the case in paragraphs 80–84 above, then proposed~~ so s 61 is ~~for this reason~~ incompatible with EU law in the respects set out above.

(c) ~~Proposed s~~Section 61A empowers relevant public authorities to authorise the acquisition of communications data (alternatively events data) without prior independent authorisation whenever a designated senior officer considers that "*there is an urgent need to obtain the data*". "*Urgent need*" is not further defined in the ~~draft regulations (nor in the~~ Act~~)~~. There is no provision for any review of the decision that there was an urgent need. Accordingly, ~~proposed~~

s 61A is not in substance and in practice limited to "*cases of validly established urgency*", as *Watson* requires (see paragraph 102(2)(b)–(c) above), and is therefore incompatible with EU law.

(d) The ~~draft~~ regulations ~~do~~ did not introduce any requirement to keep retained communications data (alternatively events data) within the EU, and for that reason Part 4 ~~will~~ remains incompatible with EU law ~~even if they are made~~ (see paragraph 174(5) above).

(e) The ~~draft~~ regulations ~~do~~ did not introduce any requirement to notify persons after communications data (alternatively events data) relating to them has been accessed or used, and for that reason Part 4 ~~will~~ remains incompatible with EU law ~~even if they are made~~ (see paragraph 174(4) above) .

(ba) Non-compliance in respect of all purposes with the CFR requirements for sufficient and detailed safeguards equivalent to those under the ECHR

177B. Further or alternatively, Parts 3 and 4, in respect of all purposes for which data may be retained, and obtained, used and/or otherwise processed, do not comply with the requirements of ECHR Articles 8 and 10 for secret surveillance regimes as set out in paragraphs 179–187 below (and further in the Claimant's Skeleton Argument dated 10 May 2019 before the Divisional Court and the Skeleton Argument of National Union of Journalists dated 10 May 2019). As CFR Articles 7, 8 and 11 provide at least equivalent protection, Parts 3 and 4 are also to at least that extent incompatible with those provisions and accordingly incompatible with EU law.

(c) CFR Articles 7 and 11 and lawyer–client communications

178. Liberty repeats paragraph 188 below by reference to CFR Articles 7 and 11.

(2) Incompatibility with ECHR

(a) Absence of individual targeting and reasonable suspicion

179. The power to issue retention notices under Part 4 (read with the Part 3 access regime) is incompatible with Articles 8 and 10 ECHR because these notices, which require retention of communications data, are not:

(1) limited by reference to an individual/set of premises ~~(or an individual operation or investigation)~~; and/or

(2) alternatively, permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

(b) Consideration of critical factors

180. Further or alternatively, the power to issue retention notices under Part 4 (read with the Part 3 access regime) is incompatible with Articles 8 and 10 ECHR because it lacks sufficient safeguards, detail and clarity as to each of the critical features (and, further, the critical features taken together) in the following respects:

181. **Scope of application:** Part 4 is of its nature a general and indiscriminate retention provision, as explained above.

(1) As explained in paragraph 126(3) above, it is not clear from the definitions in s 261 of the Act what is "*content*" (that is, the "*meaning*" of a communication under s 261(6)) in the context of videos, pictures and other communications without clear meaning.[196a] The scope of capture authorised is thus itself ambiguous.

(2) The purposes of retention are also extensive and not limited to protection of important interests. Data may be retained under Part 4 and obtained by an RPA under Part 3 for any of the manifold purposes in s 61(7) or those that are proposed to be inserted into s 87(1) (set out in paragraph 170(2) above). They are wide-

[196a] CD CoP [2.19] exacerbates this ambiguity. It states that communications data "*excludes anything within a communication including text, audio and video* ***that reveals the meaning****, other than inferred meaning, of the communication.*" Accordingly, it simply restates the definition in s 261(6) and expressly envisages that there can be text, audio or video within a communication that **do not** reveal its meaning.

ranging and not limited to serious instances of the imperilment of those interests (for example, communications data may be obtained for the purposes of preventing and or detecting any crime and any disorder).[196b] As set out above, s 87(2)(b) expressly envisages that a retention notice may "*require the retention of all data*". Further, CD CoP [17.15] envisages that multiple telecommunications operators may be covered by one retention notice. It is inevitable that, under Part 4, a large amount of clearly irrelevant data will be retained. CD CoP [17.7] rightly recognises that retention notices under Part 4 may result in the same data being retained by multiple telecommunications operators, increasing the severity of the interference.[196c] In addition, under Part 3, data must be obtained for a specific operation/investigation. This is not defined, so the concept leaves discretion to the executive about what requests for communications data can be combined.

(3) Part 3 has a prospective application — it can be used to obtain or require TOs to obtain and disclose CD as and when it is generated. Part 4 is also both retrospective (applying to data already in a telecommunications operator's possession) and prospective (requiring future retention) in its application. Further, under Part 4 (s 87(9)(b)), a telecommunications operator may be required to generate communications data it would not otherwise generate (and may under s 249(7) be compensated for this and other steps taken to comply with Part 4 retention notices). CD CoP [22.17] purports to require that a retention notice specifies the level of contribution to the costs of compliance that the government will make, and [22.2] and [22.12] make clear that the government will contribute both to the costs of retaining communications data and providing it on demand.

(4) A wide array of relevant public authorities are, under Part 3, empowered to access data including that retained under Part 4.

[196b] ~~After~~With the ~~proposed~~ amendments, this is~~will be~~ the case in relation to retention of "*entity data*", but a more limited crime purpose ~~will~~ applies~~y~~ in respect of "*events data*", as set out in paragraph 170(2) above. This ~~will~~ adds further complexity and potential confusion to the operation of Part 4.

[196c] The aspiration in CD CoP [17.7] that the Home Office will "*agree an approach*" with companies subject to the same retention notice where this possibility exists does not increase the certainty of the provisions because: it appears to apply only where the companies are covered by the same retention notice (but does not require that companies that may hold similar data are always covered by the same notice); it does not require an agreement in all cases where multiple retention is possible; and, in any event, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

(5) There is no geographical limitation nor, as mentioned, any requirement ~~(beyond the operation/investigation criterion)~~ for an individualised targeting or any requirement for reasonable suspicion before data is retained under Part 4 or any such requirement beyond the operation/investigation criterion for access to retained data ~~obtained~~ under Part 3.

182. **Duration:**

(1) A retention notice itself under Part 4 apparently remains in force indefinitely. Although it must be kept under review and there is power to revoke it (ss 90(13), 94(13)–(16)), there is no duty to cancel/revoke a retention notice, for example, if the conditions in s 87 are no longer satisfied.[196d] A retention notice may not authorise retention of data for more than 12 months, broadly from the day the data is first received (s 87(3)).[196e] However, if the retained communications data is made into a bulk personal dataset under Part 7 (or becomes subject also to a bulk acquisition warrant under Part 6 Chapter 2), it may be retained for a longer period.

(2) An authorisation under Part 3 ceases after a month (s 65(1)), subject to renewal (s 65(2)). However, ~~N~~notices to telecommunications operators (for example, requiring them to provide communications data on an ongoing basis) stay in effect

---

[196d] The purported requirement in CD CoP [18.19] to revoke a retention notice "*if it is no longer necessary*" does not contribute to the certainty of the duration of a notice because: it does not require revocation where a notice is no longer proportionate; it does not state who (which person) must do this, with what regularity, by what means or on the basis of what materials; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Indeed, CD CoP [18.3] adds further ambiguity in that it states that a review "*will take place at least once every two years once capabilities are in place*" but immediately qualifies this by saying that "*the exact timing of the review is at the Secretary of State's discretion*" (and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above)).

[196e] CD CoP [17.39] purports to authorise the retention of internet communications which "*remain active for days, or even months*" for greater than 12 months by its provision, inconsistently with s 87(3), that "[i]*n such cases the retention period commences on the day on which the communication ends*". As such data is "events data", s 87(3)(a) or (c) (whichever applies) make clear that the retention period starts from when the communication begins or the telecommunication operator first holds data (which come to the same thing). More generally, the CD CoP contains no provisions to limit discretion in setting retention periods (compare CD CoP [17.35]–[17.36], which restate this discretion). Further, CD CoP [24.12] purports to require telecommunications operators to retain for two years **from disclosure** any communications data that they disclose to a relevant public authority (it says telecommunication operators should retain "*data that was disclosed*" or other records). CD CoP [24.13] states: "*A requirement to delete data at the end of the period of its retention specified under a retention notice does not apply to records held for this purpose.*" However, there is no basis for this purported general requirement, which is contrary to ss 87(3) and 92(2).

even after an authorisation has ceased, and cease to have effect only if the authorisation is cancelled (s 65(7)). Accordingly, the Act permits a notice to be left in place where an authorisation has lapsed. The designated senior officer ("**DSO**") who granted it must cancel it if they consider that Part 3 would no longer permit the equivalent authorisation (s 65(4)), but there is no statutory duty to keep a notice under review.

183. **Authorisation procedure:**

(1) Under Part 4, a Judicial Commissioner approves the retention notice and reviews the Secretary of State's conclusions on necessity/proportionality (ss 87(1)(b), 89(1)).[196f] However, the Judicial Commissioner applies only a judicial review standard without reasons for/opposition to the decision (s 89(2)).[196g] The telecommunications operator can also refer the notice back to the Secretary of State for reconsideration (ss 90–1).

(2) In relation to access under Part 3, authorisations are not as the Act stands made or verified independently but instead by a designated senior officer at the relevant public authorities that seeks the communications data in question, save for local authorities, where justices of the peace must approve an authorisation (ss 61, 75). Most relevant public authorities therefore have no independent, external verification of the surveillance request. The requirements (1) to consult with a single point of contact (s 76) or (2) that the DSO must be independent of the investigation in question (s 63(1)) does not create any sufficient supervision, and the latter requirement is in any case qualified so as not to apply in what the DSO considers to be "*exceptional circumstances*", which include that the public body is small (s 63(2)). A Judicial Commissioner must approve any request for the purpose

[196f] Neither the Act nor the CD CoP requires any particular application or information to be presented to the Secretary of State. While they require the Secretary of State to consult with potential recipients of a notice and require or permit them to take certain matters into account (eg CD CoP [17.16]–[17.21]), provisions such as these do not meaningfully limit the Secretary of State's discretion. In particular the provisions in the CD CoP are permissive and vague and, insofar as the Act does not require any matter to be considered, these are not a statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[196g] The CD CoP does nothing to increase the certainty of this process. For example, there is no provision in the Act or the CD CoP for the Judicial Commissioner to be given any particular materials (such as those which the Secretary of State considered). CD CoP [17.24] emphasises the ambiguity of this procedure, in that it envisages that a Judicial Commissioner might "*provide oral approval to give a* [retention] *notice*".

of identifying/confirming a source of journalistic information except where an imminent threat to life exists (s 77), as explained below. Even ~~if~~with the ~~proposed~~ amendments to the Act ~~are made~~:

(a) It ~~will~~ remains the case that certain designated senior officers (who are not independent of the relevant public authority) may authorise the acquisition of retained communications data (see the proposed ss 60(7)–(7A), 70(5A) and the proposed Table in Part 1 of Schedule 4); and

(b) ~~Proposed s~~Section 61A (with s 65(3A)) empowers relevant public authorities to acquire communications data without prior independent authorisation where there is "*an urgent need to obtain the data*" for up to three business days (see paragraph 177A(3)(c) above). However, the draft regulations do not define the circumstances in which this applies,[196h] contain no mechanism for review of a decision whether an "urgent need" in fact existed, and make no provision for consequences of misuse of this further (proposed) discretion.

(3) In addition, a TCN can require a telecommunications operator to install equipment provided by the Secretary of State to obtain or disclose communications data (see paragraph 84(1A)(c)(ii)(F) above), which may prevent the telecommunications operator from supervising whether communications data is being obtained or disclosed in accordance with an authorisation.

184. **Procedure for use/examination/storage and precautions when communicating:** Part 4 requires telecommunications operators to preserve the integrity and security of the data and to destroy it if its retention ceases to be authorised (s 92). However, these provisions are general and give telecommunications operators significant discretion as to their actions.[196i] Their generality makes them hard to enforce in practice. Part 3 does

[196h] CD CoP [5.28]–[5.40] do not materially increate the certainty of the urgency procedure under s 61A because: they do not contain any further definition of "urgent need" but, instead, give examples which are in some cases very broad (see, for example, at [5.31]: "an urgent operational requirement where, within no more than 48 hours of the urgent authorisation being granted … that operational opportunity will be lost"); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[196i] The provision in CD CoP [17.33] that retention notices may include further requirements in relation to the "*generation and processing*" of retained data does not materially increase the certainty of Part 4 because it: does not require (but merely permits) the imposition of such requirements; and, in any case, it is not a

contain some safeguards for the retention, holding or destruction of data obtained by a relevant public authority.[196j] Nonetheless, ~~I~~it ~~therefore~~ fails to minimise the risk of unauthorised access or disclosure or to require proper records to be kept, and does not prevent acquired communications data being used for purposes other than that for which it was acquired.

185. **Circumstances of destruction:** As mentioned, Part 4 requires deletion of data after 12 months (or a shorter maximum time specified in a ~~warrant~~notice) (s 92(2)), subject to captured communications data being retained under Part 7 or Part 6 Chapter 2. As Part 3 contains no safeguards in this regard, it fails to ensure data is destroyed when it is no longer necessary or proportionate to hold it.[196k]

186. **Notification and remedies:** Notification is very rarely required under the Act and, where required, in the IPCr's discretion, and the ability to apply to the IPT for investigation is

---

statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Similarly, the purported requirements in CD CoP [19.10]–[19.13], [19.14]–[19.18] and [19.21]–[19.42] that telecommunications operations should put in place various kind of security measures (including security clearances and access controls), that the integrity of data should be maintained, that various systems should be secure in different ways, and that checks/audits should occur do not meaningfully add to the certainty of the procedure for use and destruction because: they are vague (so it is not possible to conclude that they are meaningful requirements) and subjective standards (for example, they include that "[m]*easures should be implemented to prevent unauthorised disclosure or processing of data*"); CD CoP [19.12] makes clear that there is no requirement to follow them or any of them; and, in any case, they are not statutory requirements so do not of their nature bind a telecommunications operator. The same is true of the requirement at CD CoP [19.43] that "[a] *system must be set up such that it is verifiable that data is deleted and inaccessible at the end of the retention period*". Insofar as CD CoP [20.4] purports to confer on the Home Office power to authorise the use of retained communications data (where a telecommunications operator does not retain it other than for the purposes of a retention notice) for purposes other than those expressly permitted by the Act, it is contrary to law. Data retained pursuant to a retention notice in these circumstances many only be used for the statutory purposes for which it is retained, that is, as the Act provides. The purported requirements in CD CoP [19.51]–[19.52] to hold retained data in the EU (if generated and processed there) or outside the EU (if generated and processed there), subject to various exception, do not meaningfully constrain a telecommunications operator's actions because they are not statutory requirements and therefore of their nature does not bind a telecommunications operator.

[196j] The "general safeguards" in CD CoP [13.1]–[13.13] do not materially increase the certainty of the procedure for use, examination, storage and communication because: they are vague, permissive and hortatory; and they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above). CD CoP [13.11] appears to permit retention and use of acquired communications data for any statutory purpose, regardless of the purpose for which it was initially acquired (and there is no statutory prohibition on this).

[196k] CD CoP [13.10]–[13.11] do not materially increase the certainty of the circumstances of destruction, because: they are vague, providing relevantly that data may be held so long as the public authority "*is satisfied that it is still necessary for a statutory purpose*" and that the retention of data should be reviewed, without further guidance; and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

a far weaker safeguard than previously thought (see paragraphs 115–116 above). In particular, the CD CoP is ambiguous as to whether it includes a definition of "relevant error".[1961] If it does not (as appears to be the case), it has the effect that there are no "serious error" errors in relation to communications data retention under Part 4 or its acquisition under Part 3 that may be informed by the IPCr to a person under s 231 (because a "*serious error*" must be a "*relevant error*": s 231(1), (9)(b)).

187. For the foregoing reasons, the retention notice regime under Part 4 (read with the Part 3 access regime) is not "in accordance with the law" or "provided by law" and/or not "necessary in a democratic society" under Articles 8 and 10 ECHR.

(c) ECHR Articles 8 and 10 and lawyer–client communications

188. It is possible to ascertain the existence of and information about lawyer–client communications from communications data, for example, whether, when and for how long a lawyer and client have spoken or otherwise communicated. That information may on occasion be sensitive or confidential. Nonetheless, Part 3 (which provides for access to communications data retained under Part 4) and, as explained in paragraph 134 above, Part 6 Chapter 2 make no provision in relation to privileged material or other lawyer–client communications. Further, the CD CoP says (relevantly) only that applicants must give "*special consideration to necessity and proportionality*" and an authorising person must take "*particular care*" where an application for communications data relates to a person known to be in various groups that include lawyers, and that legally privileged

[1961] CD CoP [24.24] states (promisingly): "*A 'reportable error' made by a public authority as set out in paragraph 24.25 of this code constitutes a relevant error for the purposes of section 231 of the Act.*" However, [24.25] then states (emphasis added): "*This section of the code **cannot** provide an exhaustive list of possible causes of reportable or recordable errors.*" It then says that "[e]*xamples **could** include*", and lists various causes of errors under a heading "*Reportable errors*" and further causes under the heading "*Recordable errors*". It is therefore unclear whether the CD CoP purports to define relevant errors or merely includes examples of possible causes of errors. Even assuming it does define (or is to be construed as defining) such errors, it is extremely narrow, **excluding** the following serious invasions of privacy (as merely "recordable" but apparently not "reportable" ie "relevant" errors): "*failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation*", "*failure to cancel a requirement to acquire or obtain data as soon as possible once it is known to be no longer valid*", "*failure to serve written notice (or where appropriate an authorisation) upon a telecommunications operator or postal operator within one working day of urgent oral notice being given or an urgent oral authorisation granted*", and "*human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed*".

material is an example of sensitive information.[196m] Accordingly, Part 4 (with Part 3 and Part 6 Chapter 2) are incompatible with Articles 8 and 10 ECHR in that they fail to provide for any of the four requirements set out in paragraph 71 above.

I GROUNDS OF CHALLENGE: BULK PERSONAL DATASETS (PART 7)

189. A brief overview of Part 7 is at paragraph 18(6) above. It empowers the Secretary of State to issue bulk personal dataset warrants or "**BPD warrants**", which permit the intelligence services to exercise their powers to retain those datasets. "Class BPD warrants" authorise retention of datasets meeting a class description and "specific BDP warrants" authorise retention of one identified dataset (s 200(3)). In broad summary:

(1) A "bulk personal dataset" is a set of information including personal data,[197] obtained by an intelligence service, whose nature is such that "*the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service*", and which is held electronically for analysis (s 199(1));

(2) An intelligence service may retain and examine a bulk personal dataset only by authority of a BPD warrant authorising retention and/or examination (s 200). This does not apply to a bulk personal dataset collected under the Act, to which Part 7 does not apply unless the Secretary of State directs otherwise (ss 201, 225);

(3) The Secretary of State may issue a BPD warrant to the head of an intelligence service if she considers it necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom insofar as those interests are also relevant to the interests of national security and proportionate (ss 204(3), 205(6));

(4) Where a BPD warrant authorises examination of the dataset, the BPD warrant must specify "operational purposes" and (i) each must be one that is or may be a purpose for which examination of the dataset is necessary and (ii) the examination of datasets for each such purpose must be necessary on the grounds on which the warrant is necessary (eg national security) (ss 204(3), 205(6), 212) — these are

[196m] CD CoP [8.8]–[8.11].

[197] As defined in the Data Protection Act 1998 but including also data about deceased persons: s 199(2).

again purposes maintained in a list by the heads of the intelligence services, which must be specified in a "greater level of detail" than the grounds mentioned in paragraph 189(3) above, for which examination may be necessary.

190. Liberty has explained above that Part 7 gives the Secretary of State the ability, through discretion, to disapply altogether safeguards in the impugned provisions, undermining their efficacy as safeguards and thus forming part of the analysis of those other provisions. Examples of safeguards that may be disapplied under s 225 if the material obtained throughresults of surveillance are made into a bulk personal dataset are:

(1) statutory requirements for arrangements that minimise the distribution and copying of intercept material, information or communications data (for example, s 150);

(2) prohibitions on selection of examination using criteria referable to people known to be in the British Islands for the purpose of intercepting their communications or obtaining their information (for example, s 152); and

(3) protections for journalistic sources (for example, s 154).

191. Additionally, Part 7, is in its own right incompatible with ECHR Articles 8 and 10 and with EU law, as explained below.

(1) Incompatibility with ECHR

(a) Absence of individual targeting and reasonable suspicion

192. The same strict foreseeability requirements as apply to secret surveillance legislation apply also to the activities of states in gathering information on individuals (see paragraph 64 above). The power to issue BPD warrants is incompatible with Articles 8 and 10 ECHR because these warrants are not:

(1) limited by reference to an individual/set of premises (or an individual operation or investigation); and/or

(2) alternatively, permitted only where there is some factual basis to suspect an identified individual of wrongdoing (or otherwise endangering national security).

(b) Consideration of critical factors

193. ~~Further or alternatively, t~~The power to issue BPD warrants is incompatible with Articles 8 and 10 ECHR because it lacks sufficient safeguards, detail and clarity as to each of the critical features (and, further, the critical features taken together) in the following respects:

194. **Scope of application:** The scope of application of the bulk personal dataset regime is largely undefined, unclear and extremely wide. Part 7 does not deal with the obtaining of a bulk personal dataset.[197a] It therefore does not constrain the intelligence agencies' discretion in this regard. Insofar as Part 7 applies to a dataset that has already been obtained, ~~V~~virtually any data could be retained and examined under a bulk personal dataset, so long as some part of the set is personal data.

(1) Bulk personal datasets must by definition contain personal data relating to individuals most of whom are not and unlikely to become of interest to the intelligence services (s 199(1)), but may contain other data also. The specific BPD warrant regime expressly applies to health records (s 206), datasets collected under the Act (s 225), and legally privileged material (ss 222–3) — with particular restrictions — but these are merely examples of content that could be included. There is no limit to the kind and nature of data that may be retained.

(2) The persons whose data may be retained or the reasons for which data may be retained are similarly unlimited (in the latter case, beyond the broad limits of the grounds for warrants — national security, serious crime and economic well-being[198] —, the operational purposes for examination of the datasets, and the similar and broad functions of the intelligence services themselves).[199] In particular, there is no link required between an individual and/or conduct and the basis for~~what triggers~~ data retention — indeed, section 199(1)(b) requires the

---

[197a] BPD CoP [4.31] confirms this: "*Part 7 does not regulate a technique for acquiring information …*".

[198] The economic well-being of the United Kingdom insofar as it is relevant to the interests of national security is in this context wider than elsewhere. Sections 204 and 205 lack the qualification in other provisions that the economic well-being of the United Kingdom may be relied upon only where the authorised conduct is necessary for the purpose of obtaining information relating to the acts or intentions of persons outside the British Islands (for example, s 102(5)–(6) in the context of targeted equipment interference warrants).

[199] The functions of the Secret Intelligence Service are set out in Intelligence Services Act 1994 s 1 and the functions of GCHQ are in s 3. The functions of the Security Service are set out in Security Service Act 1989 s 1(2)–(4).

opposite, in that most persons whose data is in~~members of~~ the set must not be "*of interest*" to the intelligence services or anticipated to become so.

(2A) Specific and class BPD warrants permit, but do not require, retention of bulk personal datasets, which creates further discretion for the executive.

(3) Operational purposes do not limit the initial retaining~~obtaining~~ of ~~communications~~ bulk personal datasets or their further disclosure (or use other than for "examination") at all.~~;~~ Further, they do little to circumscribe executive discretion in "examination" because: the operational purposes are those for which it is considered that examination is or **may be** necessary when the warrant is issued (ss 204(3)(c)(ii), 205(6)(c)(ii)); they are not required to be published; they must under s 212(8) be specified "*in a greater level of detail*" than the purposes in ss 204(3)(a) or 205(6)(a) (but this is an undemanding standard);[199a] warrants may (and will) contain all operational purposes for which all bulk personal datasets may be examined at the time (as s 212(~~63~~) ~~(12)~~ expressly permits) ~~(see paragraph 110(6) above)~~. The BCD CoP confirms this.[199b] (Further, if the operational purposes are not published, neither their existence nor their content may be taken into account in assessing the critical features: see paragraphs 45–46B above.)

(3A) Further, there is no statutory restriction on examination using criteria referable to individuals in the British Islands, so as to obtain their data or otherwise (as there is for bulk interception warrants and bulk equipment interference warrants). Instead, s 207 creates a (further) discretion, but no requirement, in the Secretary of State to impose conditions which must be satisfied where "protected data" in a bulk personal dataset held under a specific BPD warrant (but not a class BPD warrant)

[199a] The purported additional requirements in BCD CoP [5.11] that operational purposes must "*describe a clear requirement*" and "*contain sufficient detail to satisfy the Secretary of State that the BPD may only be examined for specific reasons*" add nothing because: they are vague and subjective (and gloss s 212(8)); and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[199b] BCD CoP [5.15]: "*Other than in exceptional circumstances, it will always be necessary for every BPD warrant application to require the full range of operational purposes to be specified in relation to the selection for examination of data contained in the BPD authorised under the warrant.*"

is to be "selected for examination" on the basis of criteria referable to an individual known to be in the British Islands.[199c]

(3B) Class BPD warrants authorise the retention of "*any bulk personal dataset of a class described in the warrant*": s 200(2)(a). The provisions enabling Class BPD warrants therefore: themselves create discretion as to whether a class or specific warrant is used;[199d] and enable instruments (class warrants) to be issued that create further executive discretion, that will be exercised entirely in secret, both (i) as to whether a dataset falls within a class (with no statutory requirement as to how precisely that class is defined — see s 204(2)(a) and 212(3))[199e] and (ii) whether to retain and/or examine a dataset that falls within that class.

195. **Duration:**

[199c] BCD CoP [4.31]–[4.55] purports to set out a "*scheme*" that enables the Secretary of State to impose "*additional controls*" in relation to "*selection for examination*" of protected data in a bulk personal dataset relating to an individual who is known to be in the British Islands at the time of the selection (see [4.36]). However, these provisions do not materially increase the certainty of the exercise of the broad statutory discretion because they: are general, vague and permissive (for example, [4.53] lists various conditions that might be imposed, without explaining what conditions would be appropriate in what circumstances); they purport to gloss the discretion in s 207 (for example, [4.52] suggests conditions should be imposed only where data is to be selected for examination using crtieria referable to an individual in the British Islands **and** the purpose of using those criteria is to identify protected data relating to that individual); and, in any case, this "*scheme*" is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[199d] The purported requirement in BCD CoP [5.2] that the Secretary of State not issue a class BPD warrant unless satisfied that it will be possible for the Secretary of State and Judicial Commissioner to exercise effective oversight of the operation of the warrant and retention and use of the individual BPDs authorised by it does not add materially to the certainty of the scope of class warrants because: it is a subjective, vague and speculative standard; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). Further, the purported requirements in BCD CoP [6.1]–[6.6] that each intelligence service "*should*" have a "*formal internal authorisation procedure*" by which a bulk personal dataset is retained under a class BPD warrant and as to elements that may form part of that procedure do not materially reduce the scope of discretion because they are: vague and general as to what procedure is to be followed; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[199e] Section s 202 limits the data that may be included in a bulk personal dataset held under a class BPD warrant. Section 202(3) provides that a bulk personal dataset may not be retained and/or examined where the head of the intelligence service considers that its creation or nature "*raises novel or contentions issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application by the head of the intelligence service for a specific BPD warrant*". This creates a wide and subjective discretion. Section 202(1)–(2) provide that a bulk personal dataset may not be retained and/or examined under a class BPD warrant where it includes "*protected data*" (as defined in s 203), where it includes "*health records*" (as defined in s 202(4)) and where a "*substantial proportion*" of the dataset consists of "*sensitive personal data*".

(1) The duration of a non-urgent BPD warrant is six months and conditions for renewal are substantially the same as those for issue (ss 213–14)~~., and t~~There is a duty to cancel warrants no longer considered necessary or proportionate (s 218(2)–(3)) and to remove an unnecessary operational purpose from an extant warrant (s 215(8)). However, there is no statutory duty upon the Secretary of State or a senior official to keep specific or class BPD warrants under review.[199f]

(2) In any event~~However~~, under section 219, if a bulk personal dataset warrant is cancelled or expires, an intelligence service can continue to examine the dataset – freed from the operational purposes in that warrant – in any case for five days and thereafter so long as it has an application for another warrant pending or the Secretary of State grants an extension. Further, section 219(3)(b), under which the Secretary of State may grant~~s~~ and the Judicial Commissioner may approve~~s~~ an authorisation for continued use for up to three months where the head of the intelligence service wishes to give further consideration to whether to retain the dataset (s 219(2)(b)), does not require that retention or examination be considered necessary or proportionate. This undermines the safeguard of the six-month duration of a BPD warrant and creates the possibility of abuse.

196. **Authorisation procedure:** A Judicial Commissioner must approve the Secretary of State's decision to approve a warrant, but the Judicial Commissioner applies only a judicial review standard where there ~~we~~are no reasons for the decision and there is no opposition presented to the decision (see paragraph 112(1) above).[199g] ~~and u~~Urgent

---

[199f] The purported requirement upon intercepting authorities (not the Secretary of State) to keep warrants under review in BCD CoP [5.62] does not contribute to the certainty of the duration of a warrant because: it does not state who (which person) must do this, with what regularity, by what means or on the basis of what materials; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[199g] Further, the purported requirement in BCD CoP [4.4] that there is a review within the agency prior to an application being made does not increase the certainty of the authorisation procedure because: there is no requirement for the reviewer to be independent from the person or team seeking the authorisation; the reviewer is not empowered to prevent an application if they consider that an application is not necessary or proportionate or "examination" would not be necessary for an operational purpose; and, in any case, it is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above). The purported requirements for applications at BCD CoP [4.10], [4.19]–[4.30] and [4.47]–[4.48] do not materially increase the certainty of the authorisation procedure because: do not increase the certainty of the authorisation procedure because: they do not state that an application may not be made if it does not include (a satisfactory) explanation of any of the matters referred to (and do not make any other provision for this circumstance); and, in any case, this is not a statutory requirement so may be departed from if there

warrants, valid for at least three business days, may be issued without prior Judicial Commissioner approval (ss 205(6)(e), 209), and there is no statutory definition of "urgency".[199h] Further, an operational purpose may be added or varied by a modification (s 215(2)), which enables a dataset to be examined for a purpose other than that for which it could have been examined when initially retained;[199i] and modifications adding or varying an operational purpose may be made urgently without prior Judicial Commissioner approval (ss 215(5)–(8), 217) and non-approval of the modification by a Judicial Commissioner does not affect the lawfulness of conduct carried out under it (s 217(5)).

197. **Procedure for use/examination/storage and precautions when communicating:** To issue BPD warrants, the Secretary of State must consider that the arrangements for storing and protecting them from unauthorised disclosure are satisfactory (ss 204(3)(d), 205(6)(d)).[199j] However, Part 7 provides no further detail on what this requires~~is~~. In addition, the Secretary of State must ensure that, where a warrant authorises "examination" of the bulk personal dataset, arrangements are in place such that any "examination" ~~must~~ occurs for ~~the~~ operational purposes and is necessary and proportionate (s 221).~~;~~ ~~bBut a~~As explained in paragraph 194(3) above, operational purposes are ~~this is~~ a weak safeguard. Accordingly, Part 7 makes no provision at all as to

---

are cogent reasons to do so (see paragraph 61 above). The purported requirement that a Judicial Commissioner has access to the same application as the Secretary of State in BCD CoP [4.2] and [5.28] also does not increase the certainty of the authorisation procedure because: there is no provision that a Judicial Commissioner may not approve a warrant if this is not the case; and, in any case, this is not a statutory requirement so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[199h] BCD CoP [5.34] states that urgency is determined by "*whether it would be reasonably practicable to seek the Judicial Commissioner's approval to issue the warrant in the requisite time*" and states that "[t]*he requisite time requisite time would reflect when the authorisation needs to be in place to meet an operational or investigative need*", which is vague and indeterminate. It goes on to say that an urgent situation "*should fall into at least one of the following three categories*", namely, "[i]*mminent threat to life or serious harm*", "*a significant intelligence-gathering opportunity*" or "*a significant investigative opportunity*", which are again indeterminate categories. In any case, these definitions are not a statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

[199i] As stated in BPD CoP [5.43].

[199j] The purported requirements in BCD CoP [7.3]–[7.10] and [7.50]–[7.57] in relation to retention, dissemination, copying, storage and destruction of bulk personal datasets do not materially add to the statutory provisions themselves because they are: vague, general and subjective (for example, [7.53] states that each agency should "*regularly review*" whether retention remains necessary and proportionate and [7.56] states that agencies should "*put in place an effective system*" to ensure amongst other things "*that any disclosure is properly justified*"); and, in any case, they are not statutory requirements so may be departed from if there are cogent reasons to do so (see paragraph 61 above).

the use of a retained bulk personal dataset (aside from where that use is examination which a warrant authorises). In particular, it appears that Part 7 does not regulate the manipulation and analysis nor the disclosure[199k] of a bulk personal dataset or the disclosure of information derived from it (so long as this occurs without an individual "examining" the dataset).

198. **Circumstances of destruction:** Part 7 does not expressly require destruction of a bulk personal dataset (or copies of any material obtained or derived from it) when it~~material~~ is no longer necessary or proportionate to retain that dataset (or arrangements to secure this) — see s 218. The Secretary of State or a senior official must cancel a warrant where it is no longer considered necessary or proportionate or where examination is no longer necessary for any of the operational purposes specified in the warrant (s 218(2)–(3)). ~~Further~~However, the "overrun" provision discussed above (s 219 — see paragraph 195(2) above) means that, even if a BPD warrant is cancelled, the intelligence agency may retain it and continue to examine it for five working days and thereafter as long as it has applied ~~and apply~~ for a further warrant.

199. **Notification and remedies:** Notification is very rarely required under the Act[199l] and, where required, in the IPCr's discretion, and the ability to apply to the IPT for investigation is a far weaker safeguard than previously thought (see paragraphs 115–116 above).

200. For the foregoing reasons, the bulk personal datasets provisions in Part 7 confer a wide and relatively unfettered discretion on the executive and are not "in accordance with the law" or "provided by law" and/or not "necessary in a democratic society" under Articles 8 and 10 ECHR.

[199k] BCD CoP [7.51] confirms that: "*Disclosure of BPDs, or information in BPDs held by an intelligence service (whether acquired under class BPD or specific BPD warrants) is not generally regulated by the IP Act.*"

[199l] BCD CoP [8.9] defines relevant error (relevantly to bulk personal datasets) as one that occurs where a bulk personal dataset has been retained or examined without lawful authority or there has been a failure to adhere to the restrictions set out on the use and disclosure of material under ss 221–223. BCD CoP [8.15] provides illustrative examples. It is unclear whether retention or examination without lawful authority includes the situation where there is a warrant ostensibly authorising the retention/examination but the retention/examination is nonetheless unlawful (for example, it is disproportionate in all the circumstances). Further, [8.15] appears to dilute the second limb of the definition with a (subjective) materiality threshold in that it gives as an example of a relevant error "*a **material** failure to adhere to the arrangements in force under section 221 of the Act*" (emphasis added).

(c) ECHR Articles 8 and 10 and journalistic protections

201. Part 7 contains no provisions directed to journalistic information, for example to prevent its (continued) use if identified as such in a bulk personal dataset. Accordingly, for the same reasons as set out in paragraph 118 above, it fails to comply with each of the three ~~alternative~~ mandatory requirements under ECHR Articles 8 and 10. It is incompatible with the ECHR also on this basis.

201A. The BCD CoP[199m] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are required,[199n] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[199o]

(d) ECHR Articles 8 and 10 and lawyer–client communications

202. Sections 222 and 223 make some provision for protection of items subject to legal privilege in bulk personal datasets during selection for examination. However, these protections are inadequate to comply with the requirements under Articles 8 and 10 ECHR (as set out in paragraph 71 above) in that they:

(1) do not apply to all lawyer–client communications but, instead, only to those items that are actually "*subject to legal privilege*" (ss 222(1), 223(1)) or which would be but are made or created with the intention of furthering a criminal purpose (s 222(9));

[199m] BCD CoP [7.38]–[7.48].

[199n] In particular, BCD CoP [7.45] purports to require only that, where an authorised person intends to select for examination data in a bulk personal dataset in order to identify or confirm the identity of a journalistic source, the approval of someone holding the rank of "*Director*" or above in the organisation must give their approval and that the public interest in requiring the selection must override any other public interest. In addition BCD CoP [7.47] states that, in cases of doubt as to the lawfulness of proposed handling or dissemination of confidential journalistic material, advice should be sought from a legal adviser within the authority. These paragraphs therefore do not require any assessment of whether material is confidential journalistic material that is independent of the executive. Further, these paragraphs do not purport to impose a requirement that an overwhelming public interest favours (further) examination, disclosure or use of the confidential journalistic information (save where the purpose of selection is obtaining confidential journalistic material).

[199o] This is so in particular in relation the purported prohibition in BCD CoP [7.45] on the authorised person selecting for examination content in order to identify or confirm the identity of a journalistic source or which is believed to be confidential journalistic material until the Director has authorised it.

(2) do not provide for who is to determine whether communications are (or are likely to be) legally privileged or for that person to be independent:[200]

(a) there is no express requirement for an independent person to determine whether the items are or are likely to be privileged or are not privileged because they were made to further a criminal purpose;[201]

(b) somebody, presumably each person who selects "*protected data*" for examination (and who is not independent), will have to have considered this to be able to seek the Secretary of State's or a senior official's approval (as required under s 222(1)–(3) and (9)–(12)) when selecting privileged items for examination, as will the addressee of a warrant (who is not independent) who alerts the IPCr that privileged material has been retained (under s 223(1));

(c) neither of the Secretary of State or a "*senior official*",[202] who determine under s 222(1)–(3) and 222(9)–(12) whether to permit the use of criteria for selection for examination (a) for the purpose of identifying items subject to legal privilege, (b) where their use is likely to identify items subject to legal privilege or (c) where the material selected (or from which the dataset was derived) was likely to have been created or held with the intention of furthering a criminal purpose, must themselves reach the conclusions in relation to privileged material required by ss 222(5) and (12), is independent (and Judicial Commissioners lack power under s 208(1) to review their conclusions under those provisions);[203]

---

200 Independence is possibly provided for by Judicial Commissioner approval in one narrow case: see n 203 below.

201 Although, in the last case, the person to whom the application is made may issue the warrant only if they consider it likely that the communications were made or other information was created with the intention of furthering a criminal purpose: s 112(13).

202 Section 226(1) defines "*senior official*" as "*a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service*".

203 Except where the Secretary of State, pursuant to s 222(2), personally decides whether criteria should be used for selection for examination, which occurs where those criteria are referable to an individual in the British Islands. Section 222(4) provides that, in such a case, the Secretary of State may approve the criteria only with the approval of a Judicial Commissioner, who under s 222(8) applies a judicial review standard. By contrast, Judicial Commissioner approval is not required where under s 222(12) the Secretary of State considers (if criteria for selection for examination are referable to an individual known to be in the British

(3) do not require an assessment of whether a communication or information is subject to strengthened protection under Articles 8 and 10 in all circumstances before it is selected for examination or retained thereafter (instead, s 222(1) and (9) require special approval of the criteria for selection for examination only where a purpose of their use is to select legally privileged items, material selected is likely to include legally privileged items, or a purpose of their use is to obtain items that would be legally privileged if not created with the intention of furthering a criminal purpose — where privileged items are otherwise obtained (for example, unexpectedly or where this was not likely), s 223(1) requires that the IPCr be informed as soon as is reasonably practicable but does not prevent any use of the item until the IPCr decides whether it should be destroyed or conditions should attach to its use under s 223(2)–(6)); and/or

(4) fail to ensure proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations except where a purpose of the warrant is to obtain items subject to legal privilege (only in this situation does s 222(1)–(7) require the Secretary of State or senior official have regard to "*the public interest in the confidentiality of items subject to legal privilege*" or whether there are "*exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria*": see s 222(1)(a), (5)(b), (6) and compare s 222(1)(b), (5)(b) and (9), (12)).

202A. The BCD CoP[203a] cannot and does not cure these defects. The relevant provisions do not address these requirements at all or do not purport to effect the safeguards that are

Islands at the time of the selection: s 222(10)) whether the data or material from which it was derived was likely to have been made or held with the intention to further a criminal purpose.

[203a] BCD CoP [7.21]–[7.37].

required,[203b] and are in any event not statutory requirements and may be departed from if there are cogent reasons to do so (see paragraph 61 above).[203c]

(2) Incompatibility with EU law

(a) General and indiscriminate retention ~~of content of communications~~

203. To the extent that Part 7 is used to retain data obtained under the other impugned provisions and otherwise, the breadth and the absence of **requirements** to limit the scope of a warrant in Part 7 mean it constitutes a regime (or part of the other regimes under the Act) that permits (or permit) ~~it constitutes part of a~~ general and indiscriminate preventative obtaining and retention of data. ~~retention regime and~~ It is incompatible with EU law because (see paragraph 120 above):

(A1) BPD warrants may be issued "in the interests of national security" (ss 204(3)(a)(i), 205(6)(a)(i))). If and insofar as this purpose is any wider than preventing the most serious threats to national security (as defined in *PI* and *La Quadrature*), it is incompatible with EU law or, alternatively, it must be construed as so limited to ensure that it is compatible with EU law[203d] (see paragraph 96B above). To the extent to which "the interests of national security" extend beyond these matters, the provisions enable the issue of warrants incapable of justification as strictly necessary (see paragraphs 91–92 and 95–96B above).

[203b] In particular, the BCD CoP does not: (1) provide for who is to determine whether communications are (likely to be) lawyer–client communications or require this to be determined by an independent person (but provides only for consultation of a legal adviser within the agency where there is doubt about privilege or "*wherever possible*" where privileged material is disseminated: BCD CoP [7.21], [7.34]); (2) require an assessment of whether a lawyer–client communication is subject to strengthened protection under Articles 8 and 10 ECHR in all circumstances before it is examined, selected for examination or further used (instead, only where privileged communications are likely to be obtained by selection for examination or it is the purpose of selection for examination to obtain them, and not before any further use: see BCD CoP [7.25]); (3) require proper consideration of the public interest in the confidentiality of lawyer–client communications in all situations where they are examined, selected for examination or used (save where it is the purpose of examined or selection for examination to obtain privileged communications, in which case the issuing authority must be satisfied that there are "*exceptional and compelling circumstances*" that make the examination or selection for examination necessary: BCD CoP [7.28]).

[203c] This applies in particular to the purported requirement in BCD CoP [7.26] not to carry out any examination or selection for examination without approval from the relevant approver where the purpose is to identify privileged communications or they are likely to be obtained.

[203d] See Case C-106/89 *Marleasing SA v La Comercial Internacional de Alimentacion SA* ECLI:EU:C:1990:395 [9].

(1) In addition, insofar as BPD warrants permit the state to **retain and access** BPDs **other** than for the purpose of preventing the most serious threats to national security, namely, ~~it is not limited to the purpose of~~ fighting serious crime or the economic purpose~~, alternatively, to serious threats to all of the interests listed in~~ (see ss 204(3)(a) and 205(6)(a)). To that extent the regime for BPD warrants is incompatible with EU law, as it constitutes a regime of general and indiscriminate retention and access other than for the purpose of preventing the most serious threats to national security. ~~and in consequence~~It allows the issue of a warrant that permits retention for purposes that are not capable of justifying such a~~n~~ serious interference with Article 7 and 8 rights~~.~~; Further, it does not limit the data obtained and retained, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period, to what is strictly necessary (see paragraphs 95–96B above).

~~(2) alternatively, to the extent that the content of communications or other information collected indiscriminately are recorded in a bulk personal dataset, forms part of an interference that affects the essence of the rights under Articles 7 and 8; and/or~~

~~(3) alternatively, forms part of a regime that permits the authorisation of the indiscriminate and general retention of communications data, and is not limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, so fails to permit retention of only that data which is strictly necessary.~~

(3) Insofar as Part 7 (read with other provisions of the Act or subordinate legislation) permits CSPs and/or the state to carry out automated processing of data, it does not contain requirements that the model or criteria be specific and reliable, non-discriminatory (including that they are not based on sensitive matters in isolation) and regularly re-examined or that any positive result is individually reviewed before action adversely affecting an individual is taken, as set out in paragraph 102B above.

(b) Non-compliance with further Watson requirements

204. To the extent that Part 7 is used to retain data obtained under the other impugned provisions, it fails to comply with the *Watson* requirements in the same manner as and for the reasons set out above in relation to each impugned provision. Further or alternatively, insofar as Part 7 otherwise permits BPDs to be retained,[203e] accessed and/or otherwise processed **other than** for the purpose of preventing the most serious threats to national security (or for operational purposes referable to those other purposes), ~~I~~it is ~~otherwise~~ incompatible with EU law because fails to comply with the *Watson* requirements in each of the following alternative respects, namely, that it:

~~(1) is not strictly limited to retaining data for defined and precise offences (nor even to retaining data for the purpose of preventing serious crime);~~

~~(2) does not ensure that retention of or continued access to data is connected to the objective pursued or depends on a link between continued access/retention and preventing serious crime (alternatively, a serious threat to national security);~~

~~(3) does not, as a general rule, limit government's access to data of individuals suspected of planning, committing, having committed or otherwise been implicated in serious crime (allowing access to the data of other persons only in a specific case and to protect vital national security, defence or public security interests);~~

~~(4) does not require a reasoned application from a national authority to request access;~~

(5) does not require judicial or independent approval each time data is accessed, on the basis of a reasoned application from a national authority to request access;

(6) does not require notification of any person affected (ie whose data has been accessed pursuant to a BPD warrant) as soon as that notification is no longer liable to jeopardise the purpose of the retention of the data; and/or

(7) does not require data to be retained in the EU.~~;~~

[203e] Read, as necessary, with the underlying powers of the Security Service (see Security Service Act 1989 ss 1–2), the Secret Intelligence Service (see Intelligence Services Act 1994 s 1–2), and GCHQ (see Intelligence Services Act 1994 s 3–4). Those powers are in each case entirely general and do not add any material qualification by way of safeguard or specificity to the power to retain a BPD.

~~(8) does not require providers of electronic communications services (if holding data retained under Part 7) to guarantee a particularly high level of protection;~~

~~(9) does not impose definitive retention periods or impose or require retention periods to be based on objective criteria or adapted depending on the usefulness of material obtained; and/or~~

~~(10) it (and the provisions in Part 8) do not require consideration by an independent authority specifically directed to compliance with the level of data protection required by EU law.~~

(ba) Non-compliance in respect of all purposes with the CFR requirements for sufficient and detailed safeguards equivalent to those under the ECHR

204A. Further or alternatively, Part 7, in respect of all purposes for which BPDs may be retained, used and/or otherwise processed, does not comply with the requirements of ECHR Articles 8 and 10 for secret surveillance regimes (of which it is part), as set out in relation to each other impugned power above, and further with the requirements for state databases as set out in paragraphs 192–200 above (and further in the Claimant's Skeleton Argument dated 10 May 2019 before the Divisional Court and the Skeleton Argument of National Union of Journalists dated 10 May 2019). As CFR Articles 7, 8 and 11 provide at least equivalent protection, Part 7 is also to at least that extent incompatible with those provisions and accordingly incompatible with EU law.

(c) CFR Articles 7 and 11 and journalistic protection / lawyer–client communications

205. Liberty repeats paragraphs 201 and 202 above by reference to CFR Articles 7 and 11.

J RELIEF

206. The Defendants ~~have~~ agreed prior to the issue of the claim that Liberty should file and serve an application for a costs-capping order within 14 days of the decision on permission and the Defendants should have 14 days thereafter to file their reply. ~~Should permission be granted, an order is sought in these terms.~~ As set out in paragraph 29R above, a costs capping order was made on 4 October 2017. The costs capping order was varied by the consent of the parties to cover the Bulk Powers Claim (and thus the entirety

of the claim) by orders agreed on 10 December 2018. ~~Liberty intends to apply to vary the existing costs-capping order so that it applies (with appropriate provision) in respect of the Bulk Powers Claim also. It therefore invites the Court to give directions that include the service of that application within 14 days of service of the decision on permission and for the Defendants' reply within a further 14 days.~~

207. For the foregoing reasons, Liberty seeks:

(1) Orders for the disapplication of each of the impugned provisions due to (and where appropriate to the extent of) their incompatibility with EU law.[204] If and to the extent required, Liberty relies in this regard also on its right to an effective remedy under CFR Article 47.[205] Liberty recognises that, as occurred in the Divisional Court in *Watson*, an appropriate period for amendment of the Act to reflect the Court's decision should be allowed before this order takes effect, albeit the long time that has passed since the claim was brought is relevant to consideration of its length;

(1A) A declaration that, in each respect in which the Court finds that each of the impugned provisions is incompatible with EU law, it is unlawful and does not provide lawful authority for that which it purports to authorise;

(1B) An order quashing the Data Retention and Acquisition Regulations 2018 on the basis and to the extent that they are incompatible with EU law and therefore ultra vires, void and of no effect and/or a declaration to that effect;

(2) Further or alternatively, if and to the extent the impugned provisions are not (immediately) disapplied, declarations of incompatibility under s 4 of the Human Rights Act 1998, on the basis of the incompatibility with ECHR Articles 8 and/or 10 and/or 14 of each of the impugned provisions;

(3) Such further or other relief as the Court considers fit; and

(4) Costs.

---

[204] *R (Davis) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) [120]–[122] (Bean LJ).

[205] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2015] 3 WLR 409 [98] (Lord Dyson MR and Sharp LJ).

~~MARTIN CHAMBERLAIN QC~~

~~DAVID HEATON~~

~~Brick Court Chambers~~

~~28 February 2017~~

~~MARTIN CHAMBERLAIN QC~~

~~Brick Court Chambers~~

~~BEN JAFFEY QC~~

~~Blackstone Chambers~~

~~DAVID HEATON~~

~~Brick Court Chambers~~

~~29 June 2018~~

~~MARTIN CHAMBERLAIN QC~~

~~Brick Court Chambers~~

~~BEN JAFFEY QC~~

~~Blackstone Chambers~~

~~DAVID HEATON~~

~~Brick Court Chambers~~

~~3 August 2018~~

BEN JAFFEY QC

Blackstone Chambers

DAVID HEATON

Brick Court Chambers

31 December 2020

BHATT MURPHY