Neutral Citation Number: [2019] EWHC 2057 (Admin)

Case No: CO/1052/2017

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

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 29/07/2019

Before :

LORD JUSTICE SINGH
and
MR JUSTICE HOLGATE

- -

Between :

The Queen (on the Application of National Council for Civil Liberties (Liberty))	**Claimant**
- and -	
Secretary of State for the Home Department	**1st Defendant**
Secretary of State for Foreign and Commonwealth Affairs	**2nd Defendant**
National Union of Journalists	**Intervener**

- -
- -

Martin Chamberlain QC, Ben Jaffey QC and David Heaton (instructed by **Bhatt Murphy**) for the **Claimant**
Sir James Eadie QC, Gerry Facenna QC, Julian Milford and Michael Armitage (instructed by the **Government Legal Department**) for the **Defendants**
Angus McCullough QC and Rachel Toney (instructed by **SASO)** as **Special Advocates**
Jude Bunting (instructed by **Bindmans**) for the **Intervener**

Hearing dates: 17-21 June 2019

- -

Approved Judgment

Lord Justice Singh and Mr Justice Holgate:

Introduction

1. In *R (National Council for Civil Liberties) v Secretary of State for the Home Department* [2018] EWHC 975 (Admin); [2019] QB 481 this Court gave judgment on the first part of the Claimant's challenge to the Investigatory Powers Act 2016 ("the IPA" or "the 2016 Act"). That challenge was brought under European Union ("EU") law. It concerned only Part 4 of the 2016 Act, concerning powers to require the retention of "communications data", which was the relevant part which had then been brought into force. The Court is now concerned with the second part of the Claimant's challenge, which arises under the Human Rights Act 1998 ("HRA"). This challenge concerns various other parts of the 2016 Act, which have now been brought into force on various dates. The only remedy which the Claimant seeks is a declaration of incompatibility under section 4 of the HRA.

2. The Claimant challenges four different sets of provisions in the 2016 Act. What they all have in common is that they concern "bulk" powers rather than powers which are directed at any particular individual who may be a potential subject of interest (sometimes called "targeted" surveillance). The relevant provisions are as follows:

   (1) Part 6, Chapter 1, which relates to bulk interception warrants.

   (2) Part 6, Chapter 3, and Part 5: these concern warrants for bulk and thematic "equipment interference". The Claimant has described this in its submissions as

"hacking" but we think it preferable to use the term used in the IPA itself, namely "equipment interference".

(3) Part 7, which relates to warrants for bulk personal datasets ("BPD").

(4) Part 6, Chapter 2, and Parts 3-4: respectively warrants for bulk acquisition of "communications data" and retention notices for, and acquisition of, communications data. "Communications data" is not the "content" of communications but other matters such as "where, when and who".

3. In broad terms the Claimant's case is that:

(1) The provisions of the 2016 Act under challenge are incompatible with Article 8 (the right to respect for private life and correspondence) and Article 10 (the right to freedom of expression) of the European Convention on Human Rights ("ECHR") because they are too wide. They lack the "minimum safeguards" established by the European Court of Human Rights for secret surveillance regimes. They are neither necessary in a democratic society nor proportionate.

(2) Further or alternatively, the powers lack sufficient safeguards to comply with the "minimum requirements" taken together. For this reason they are said not to be "in accordance with the law" (the phrase used in Article 8) or "prescribed by law" (that used in Article 10). This was the main focus of the Claimant's submissions before us.

(3) The powers lack sufficient safeguards for lawyer-client communications and journalistic material, including the confidential sources of a journalist's information.

(4) The continued operation of Part 1, Chapter 2, of the Regulation of Investigatory Powers Act 2000 ("RIPA"), which concerns the acquisition of communications data, is not in accordance with law because it does not comply with EU law. This follows, it is said, from this Court's judgment in 2018, to which we have referred above. The Claimant submits that, although amendments were made to Parts 3-4 of the IPA in accordance with the declaration granted by this Court, the previous regime has not been repealed. The Claimant submits that that regime is not in accordance with law for the reasons identified in this Court's previous judgment.

4. This last part of the challenge, which had not been foreshadowed in the grounds but which was set out in the Claimant's skeleton argument for the substantive hearing before this Court, at paras. 163-166, was not pursued at that hearing.

5. A further ground of challenge has arisen only recently as the result of disclosures made by the Defendants pursuant to their duty of candour and co-operation with the Court. For that reason this argument could not have been foreshadowed in the Claimant's grounds of challenge. This argument is to the effect that the way in which the Security Service (MI5) has in fact operated its handling procedures in the last few years has been unlawful; and that this demonstrates that the safeguards in the IPA against the risk of abuse of power, even if they were adequate in theory, are not effective in practice.

6. There is a fundamental difference of approach as between the Claimant and the Defendants in relation to the obtaining and retention of bulk data, as distinct from its later selection for examination. It is common ground between the parties that there is an interference with the right to respect for private life at all material stages, including at the stage when data is obtained and retained. However, the Defendants submit that there is no "meaningful" intrusion into privacy rights until the stage when the data is selected for examination. The Claimant submits that that is wrong and inconsistent with "decades" of authority from the European Court of Human Rights. It also submits that this is a proposition which is not only "startling" but "dangerous and artificial".

7. The Claimant submits that the 2016 Act creates a regime in which vast amounts of data can be "hoovered up" on a bulk basis in circumstances in which most of it will never be of any interest to the intelligence agencies or other authorities, such as the police. It submits that that risks creating a society in which everyone is susceptible to surveillance but does not know when they might be subject to such surveillance. The Claimant submits that that can have a "chilling effect" on the way in which people going about their lawful business will behave, for example in the way in which they search the internet or store private information, such as diaries or photographs, on their computers or smart phones. The Claimant submits that the regime created by the 2016 Act is inconsistent with fundamental values in a free and democratic society governed by the rule of law.

8. The Defendants submit that the legislative scheme carefully created by the 2016 Act is compatible with Articles 8 and 10 and, in particular, that it is both in accordance with law and necessary in a democratic society. They submit that the Act strikes a fair balance between the rights of the individual and the general interest of the community, particularly bearing in mind, first, that it was the product of extensive pre-legislative scrutiny; and, secondly, the safeguards introduced by it, including the creation of the office of the Investigatory Powers Commissioner ("IPC").

9. The Claimant accepts that certain submissions which it makes in its pleaded grounds are inconsistent with the judgment of the European Court of Human Rights (First Section) in *Big Brother Watch & Ors v United Kingdom* (Application No 58170/13, judgment of 13 September 2018). At the request of the applicants that case has been referred to the Grand Chamber. The Grand Chamber heard that case after the hearing before this Court, on 10 July 2019, together with a case from Sweden called *Centrum för Rättvisa v Sweden* (2019) 68 EHRR 2. In those circumstances the Claimant has not argued those points before this Court but has reserved them for consideration on any appeal in this case in the light of the decision of the Grand Chamber in *Big Brother Watch*. At the hearing before us it was common ground that this Court should not delay giving its judgment pending the decision of the Grand Chamber in *Big Brother Watch*.

10. This concession is important for a proper understanding of the issues which are currently before this Court. The European Court of Human Rights has already held that at least some "bulk" powers, in particular for the collection of data by interception warrants, are in principle compatible with the ECHR. That issue of principle is therefore not in issue before this Court, although it will be before the Grand Chamber of the European Court of Human Rights. We therefore have to address the issues which do arise before this Court against that important background.

The issues which we have to address concern, in particular, whether the 2016 Act has put in place sufficient safeguards against the risk of abuse of such bulk powers, both generally and in relation to two specific areas: lawyer-client communications and journalistic material.

Procedural matters

11. On 14 June 2017 Jeremy Baker J granted permission to bring this claim for judicial review in respect of Part 4 of the IPA and stayed the remainder of the claim on the basis that it was only Part 4 which was then in force. As we have mentioned above, this Court gave judgment in relation to that part of the claim on 27 April 2018. It made a declaration that Part 4 was incompatible with EU law in two respects which were by then conceded by the Defendants and also that Part 4 had to be amended within a reasonable time, that is by 1 November 2018. This Court stayed judgment on three further alleged incompatibilities with EU law pending the decision of Court of Justice of the EU ("CJEU") in a reference which has been made by the Investigatory Powers Tribunal ("IPT") in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs (No. 2) (Note)* [2017] UKIPTrib 15_110-CH; [2018] 2 All ER 166. That reference remains pending.

12. On 31 October 2018 the Data Retention and Acquisition Regulations 2018 were made in accordance with this Court's earlier declaration in relation to EU law.

13. Codes of Practice were laid before Parliament under the IPA on 18 December 2017 and 28 June 2018. The Claimant has amended its grounds to take account of these and has also re-amended its grounds to take account of recent developments.

14. On 27 November 2018 Singh LJ gave permission to bring this claim for judicial review in relation to the remaining grounds. His order also stayed the claim insofar as it was based on EU law pending the CJEU preliminary ruling on the reference in the *Privacy International* case, a course which had been agreed by the parties.

15. On 1 May 2019 the National Union of Journalists ("NUJ") applied to intervene in this claim and permission to do so was granted by Singh LJ at a directions hearing on 10 May 2019.

16. There is before the Court an application by the Defendants under section 6 of the Justice and Security Act 2013 for the Court, if it becomes necessary to do so, to hold a closed material procedure ("CMP") in this case. We will set out later in this judgment the context in which that application has arisen. For present purposes it will suffice to say that, as things developed before and during the course of the hearing before this Court, we found it unnecessary to consider the application for a CMP or to hold a closed hearing in this case. This was the result of helpful discussions which took place between those representing the Defendants and the Special Advocates, which enabled a great deal of material to be disclosed to the Claimant and to be considered by this Court in open proceedings. We are satisfied that it is not necessary for the fair disposal of the issues in this case for the Court to consider any material which has not been made available to the Claimant and is in open.

17. We are very grateful to all concerned, including the Special Advocates, for their strenuous efforts in enabling this Court to deal with this case expeditiously and efficiently. We are grateful to all counsel for the high quality of their written and oral submissions.

Background to the 2016 Act

18. The threats to security which the United Kingdom ("UK") and members of the public face are well known and hardly need evidence, although there is plenty of such evidence which has been placed before this Court: see in particular the first witness statement of James Dix, acting Head of the Investigatory Powers Unit in the Office for Security and Counter-terrorism at the Home Office. By way of example, in 2017 there were five terrorist attacks, in London and Manchester, which resulted in 36 deaths. The organisations Daesh (sometimes called "Islamic State" or "ISIL") and al Qa'ida continue to pose threats to British nationals and others around the world. There is an increasing threat from far-right extremism. Further, this country faces "sustained hostile activity from certain states": see a speech given by the Director General of MI5 (Sir Andrew Parker) in Berlin on 14 May 2018, quoted at para. 15 of Mr Dix's first witness statement.

19. In addition, there is an acknowledged need to support the investigation and punishment of serious organised crime, including offences against children. It is also well known that those who would wish to do harm to this country and its inhabitants are increasingly able to make use of encryption and the "dark web", which Mr Dix describes, at para. 20 of his first witness statement, as "a space in which information can be exchanged anonymously beyond the reach of law enforcement."

20. Against that background, Mr Dix expresses the following opinion to this Court at para. 24 of his first witness statement:

> "The investigatory powers under challenge in this claim make a very significant contribution to tackling the kind of threats set out above: indeed, they are essential for doing so."

At para. 28 he tells this Court that the use of bulk data is among the few effective methods to counter the illicit use of the dark web. Further, as he points out at para. 29, in certain parts of the world the UK has no physical presence, so there are often no initial intelligence leads on emerging threats, whether from terrorists, serious criminals or state-based threats:

> "Bulk powers allow security and intelligence agencies to identify and map out known and evolving networks, in turn enabling further intelligence gathering on likely threats. …"

21. Finally, in this context, it is important to note that the situation can often be a "dynamic" one. At para. 30 of his first witness statement Mr Dix states that:

> "… Bulk powers also allow the security and intelligence agencies to respond at pace, quickly identifying threats and ruling individuals in or out of investigations. Bulk powers are made more important by the fact that terrorist threats are increasingly diverse in nature and can escalate with increasing speed through the use of the internet to radicalise supporters and plan and execute attacks."

22. The utility of bulk powers is illustrated by the fact that, as Mr Dix says at para. 32:

> "… Bulk data analysis has played a significant part in every major counter terrorism investigation over the last decade, including in each of the seven terrorist attack plots disrupted between 2014 and the publication of the Operational Case in 2016. …"

(That is a reference to the Government's operational case for bulk powers, which was published during the passage of the Investigatory Powers Bill.)

23. Mr Dix states at para. 33 of his first witness statement that, before the 2016 Act, many similar powers, including bulk powers, could be found in a range of different statutes, in particular the following:

(1) Powers to intercept communications, including in bulk, were provided for in Part 1, Chapter I of RIPA.

(2) Equipment interference was provided for in powers contained in the Intelligence Services Act 1994 and the Police Act 1997.

(3) Bulk personal datasets could be acquired using information gathering powers in the Intelligence Services Act 1994 ("ISA") and the Security Services Act 1989; and processes for their retention and examination were set out in published agency handling arrangements.

(4) Retention of communications data was provided for in the Data Retention and Investigatory Powers Act 2014 (as amended by the Counter-terrorism and Security Act 2015) and the Anti-terrorism, Crime and Security Act 2001.

(5) The targeted acquisition of communications data was primarily provided for in Part 1, Chapter II, of RIPA.

(6) Bulk acquisition of communications data was provided for in the Telecommunications Act 1984.

24. Prior to the Investigatory Powers Bill, Mr Dix states (at para. 34) that there were three reviews of investigatory powers undertaken. The first was 'A Question of Trust' (June 2015 by David Anderson QC, who was at that time the Independent Assessor of Terrorism Legislation and is now Lord Anderson of Ipswich QC). In March 2015 there was the 'Report on Privacy and Security' by the Intelligence and Security Committee of Parliament ("ISC"). In July 2015 there was a report by a panel convened by the Royal United Services Institute ("RUSI"). Mr Dix states that all three reviews agreed that the use of the existing complement of investigatory powers

remained vital to the UK's national security and other interests. They made 198 recommendations as to the way in which these powers should be overseen. He says, at para. 36, that the central recommendation by Lord Anderson in 'A Question of Trust' was that:

> "A comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive powers that it may be necessary for the public authorities to use." (Executive summary, para. 10)

25. During the passage of the 2016 Act through Parliament there was pre-legislative scrutiny by three committees: the House of Commons Science and Technology Committee, which produced a report entitled 'Investigatory Powers Bill: Technology Issues' in January 2016; the ISC, which produced a report on the Bill in 2016; and a report by the Joint Committee on the Bill produced in February 2016. The Joint Committee alone took 2,364 pages of written evidence and transcripts of oral evidence from stakeholders across society. The Joint Committee recommended that the Government should publish a fuller justification for each of the bulk powers alongside the Bill (recommendations 23 and 28). This was done in the Operational Case for Bulk Powers. The Government also published an amended operational case for the retention of internet connection records following a recommendation from the Joint Committee.

26. The Investigatory Powers Bill was introduced in Parliament on 1 March 2016, having been previously published in draft form for pre-legislative scrutiny. The Government published its own formal response to that scrutiny.

27. Furthermore, at the same time as the Bill was introduced, draft codes of practice were published so that Parliament would have the opportunity to consider those alongside the Bill.

28. The Government also commissioned the Independent Reviewer of Terrorism Legislation to conduct a detailed review of the operational case for bulk powers, which was published by Lord Anderson as the 'Report of the Bulk Powers Review' in August 2016.

29. The Government itself also published an operational case for use of communications data by public authorities.

30. The new regime introduced by the 2016 Act is now largely operational, with the majority of the powers under the Act having been brought into force during the course of 2018. The provisions relating to equipment interference and interception were commenced for the intelligence services on 27 June 2018, with interception for law enforcement commenced on 26 September 2018 and equipment interference on 5 December 2018. A commencement order in respect of the bulk communications data and bulk personal dataset provisions was made on 18 July 2018, and the provisions concerning the issuing of warrants came into force on 22 August 2018. The final part of the Act to be commenced was Part 3, which was commenced on 5 February 2019.

31. In the meantime, earlier, in 2017, there had been established the office of the IPC. The 2016 Act requires the IPC to be a person who holds or has held high judicial office. The first and current IPC is Sir Adrian Fulford, who is a serving Lord Justice of Appeal. He has a staff of some 50 people, including those with technical expertise. His office includes 15 Judicial Commissioners ("JCs"), who also have to be persons who hold or have held high judicial office: they include retired members of the High Court, the Court of Appeal and the Supreme Court. The IPC's deputy is Sir John Goldring, a retired member of the Court of Appeal.

32. In addition, in anticipation of the full implementation of Part 3 of the Act, which is expected to occur by the end of 2019, there has been created the Office for Communications Data Authorisations ("OCDA"), which is under the remit of the IPC.

33. In the view of many commentators the most significant and innovative provision in the 2016 Act is the creation of a "double lock" for warrants authorising use of certain intrusive powers. Where this applies the Act requires that an independent JC must approve the decision of the Secretary of State (or, where relevant, Scottish Minister/law enforcement chief). The UN Special Rapporteur on the Right to Privacy (Joseph Cannataci), following a visit to the United Kingdom, observed in his 'end of mission statement' that this element of judicial review "assisted by a better-resourced team of experienced inspectors and technology experts is one of the most significant safeguards introduced by the IPA": see his Report of June 2018, p.2.

The legislative scheme of the 2016 Act

34. The 2016 Act is inevitably a complicated piece of legislation, with many inter-locking provisions. They need to be considered in full. It would be impossible to set the full provisions out in this judgment. It would also not assist in comprehension. The parties have helpfully agreed an "overview of relevant legislation", prepared by the Defendants (with substantial input from the Claimant) and agreed by the Claimant subject to three "riders", which set out some additional points. We are grateful to the parties and annex the overview, including the points made in the Claimant's riders, to this judgment. For that reason we can be relatively brief in our outline of the legislative scheme in the 2016 Act here.

35. The 2016 Act draws a distinction between targeted warrants and bulk warrants. In this case we are principally concerned with bulk warrants.

36. A bulk interception warrant under Chapter 1 of Part 6 (section 138), or a bulk acquisition warrant for communications data (which excludes "content") under Chapter 2 of Part 6 (section 158), or a bulk equipment interference warrant under Chapter 3 of Part 6 (section 178) has to be necessary at least in the interests of national security (but may also be for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the UK insofar as those interests are also relevant to national security).

37. All three types of bulk warrant under Part 6 of the 2016 Act authorise (among other things) the selection for examination of the data to which they relate and disclosure of such material to the person named in the warrant or to any person acting on his behalf.

38. Bulk warrants are not available to public authorities generally such as the police. An application for a bulk warrant must be made by or on behalf of the head of an intelligence service: see section 138(1), section 158(1) and section 178(1).

39. The power to issue a warrant must be exercised by the Secretary of State personally: see section 141, section 160 and section 182.

40. Each type of bulk warrant must specify the "operational purposes" for which any material obtained under that warrant may be selected for examination: see section 142(3), section 161(3) and section 183(4).

41. There are detailed provisions about the making of the list of "operational purposes" by the heads of the intelligence services. An operational purpose may be specified in that list only with the approval of the Secretary of State. The list of operational purposes must be provided to the ISC every three months and must be reviewed by the Prime Minister at least once a year: see the overview at para. 34.

42. In deciding whether to issue a bulk warrant the Secretary of State must apply the principles of necessity and proportionality: see para. 31 of the overview.

43. The issuing of all three types of warrant is subject to prior approval by a JC. The JC must apply the principles of judicial review (sections 140, 159 and 179). An urgent application for a warrant for bulk equipment interference can be made (sections 180-181), in which case there is no prior approval by a JC but instead review after the warrant is issued.

44. It was common ground between the parties at the hearing before us that the principles of judicial review include for relevant purposes the legality of an interference with a Convention right under section 6(1) of the HRA; and therefore the JC must consider for himself or herself questions such as whether an interference is justified as being proportionate under Article 8(2). On behalf of the Defendants Sir James Eadie QC emphasised that that does not mean that the experience and opinion of the agencies is not to be given appropriate weight in the assessment of proportionality. That, as was common ground before us, is conventional in human rights cases of this type, for example when they are brought before this Court. Such respect is owed to those who are responsible for the maintenance of national security and the protection of the public in this country for two reasons.

45. The first is "institutional competence": the Secretary of State and the agencies and others concerned have far greater experience of dealing with these issues than a court can possibly have. The second reason is the democratic legitimacy of the Secretary of State, who is accountable to Parliament.

46. All three types of bulk warrant last for six months (sections 143, 162 and 184) unless they have already been cancelled or are renewed (sections 144, 163 and 185). Renewal is subject to approval by a JC.

47. Bulk interception warrants may cover both the "content" of communications and "secondary data". Bulk equipment interference warrants may cover both content and "equipment data", which is similar to "secondary data". These two concepts are similar to each other and include both "systems data" and in addition "identifying

data" which is capable of being separated logically from the remainder of a communication without revealing the meaning of any of the communication.

48. In the case of both bulk interception warrants and bulk equipment interference warrants, their "main purpose" must be to obtain "overseas-related communications", that is communications sent to or received by individuals outside the British Islands or also (in the case of bulk equipment interference warrants) overseas-related information or equipment data. The warrant may also authorise incidental conduct, including incidental interception (sections 136(5) and 176(5)).

49. In the case of bulk interception warrants and bulk equipment interference warrants the selection for examination of intercepted content or "protected material" is subject to what is known as the "British Islands safeguard" (sections 152(3) and (4) and 193(3) and (4)). By way of example, section 152(4) states that:

> "intercepted content may not at any time be selected for examination if –
>
> (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."

50. In contrast, bulk acquisition warrants relate to communications data and do not cover "content". Such warrants are not confined to overseas-related communications.

51. Part 7 of the Act deals with bulk personal datasets.

52. Legal professional privilege is governed by specific provisions in the Act: see sections 153, 194 and 222-223. Confidential journalistic material intercepted or obtained under a bulk interception warrant or a bulk equipment interference warrant is governed by sections 154 and 195. Additional safeguards for such material apply where targeted examination warrants are sought: see sections 27, 28, 29, 55, 113, 114 and 131.

53. It is important to note the "general duties" in relation to privacy which are to be found in section 2(2) of the 2016 Act. These duties apply to a "public authority" within the meaning of section 6 of the HRA other than a court or tribunal. It would therefore include the Secretary of State and the IPC but not the IPT. The duties apply where such a public authority is deciding whether to issue, renew or cancel a warrant under Parts 2, 5, 6 or 7; whether to approve such a decision to grant, approve or cancel an authorisation under Part 3; or to give a notice under Part 4: see section 2(1).

54. In exercising the specified functions, section 2(2) provides that the public authority "must have regard to" a number of matters which are then listed, including:

> "(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or

> notice is *higher* because of the *particular sensitivity* of that information". (Emphasis added)

55. Section 2(5) gives examples of sensitive information for these purposes, including "items subject to legal privilege" and "any information identifying or confirming a source of journalistic information".

56. There is one important aspect of the 2016 Act which is not addressed in the overview in the Annex to this judgment. This concerns the codes of practice which have been made under the Act. Section 241 gives effect to Sch. 7, which concerns those codes of practice. The Secretary of State must issue a code of practice about the exercise of relevant functions conferred by virtue of the Act: see para. 1(1) of Sch. 7.

57. Each code must include provision designed to protect the public interest in the confidentiality of sources of journalistic information; and provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds items subject to legal privilege or relevant confidential information: see para. 2(1)(a) and (b) of Sch. 7.

58. "Relevant confidential information" includes information which is held in confidence by a member of a profession and consists of "journalistic material", which would be "excluded material" as defined by section 11 of the Police and Criminal Evidence Act 1984.

59. Para. 4 of Sch. 7 provides that, before issuing a code, the Secretary of State must prepare and publish a draft of that code and consider any representations made about it: see para. 4(1). In particular, the Secretary of State must consult the IPC: see para. 4(2). A code can only come into force in accordance with regulations made by the Secretary of State; and a statutory instrument containing such regulations may not be made unless the draft has been laid before, and approved by a resolution of, each House of Parliament: see para. 4(4). In other words the affirmative resolution procedure is required.

60. Under para. 6 of Sch. 7 a person must have regard to a code when exercising any functions to which the code relates: see para. 6(1). A failure on the part of a person to comply with any provision of the code does not of itself make that person liable to criminal or civil proceedings but a code is admissible in evidence in any such proceedings: see para. 6(2) and (3). A court or tribunal may, in particular, take into account such a failure in determining a question in any such proceedings: see para. 6(4).

61. A "supervisory authority" may take into account such a failure in determining a question which arises: see para. 6(5). For this purpose "supervisory authority" includes the IPC and the IPT.

62. As was common ground before this Court, the European Court of Human Rights has long recognised that instruments such as a code of practice can be part of the overall scheme which renders any interference with a Convention right "in accordance with the law".

The Human Rights Act 1998

63. In these proceedings the Claimant relies on Articles 8 and 10 of the ECHR, which are among the Convention rights set out in Sch. 1 to the HRA.

64. Article 8 provides:

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

65. Article 10 provides:

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

66. We have emphasised the words in those two articles which lie at the heart of the issues in this case. It is common ground that the phrase "in accordance with the law" in Article 8(2) has materially the same meaning as "prescribed by law" in Article 10(2). The equivalent phrase in the French text of the ECHR (both the English and the French texts being the authoritative texts) is in fact the same in both Articles 8 and 10 ("*prévue par la loi*").

67. The main way in which the Convention rights are given effect in domestic law is through the obligation in section 6 of the HRA. Section 6(1) makes it "unlawful for a public authority to act in a way which is incompatible with a Convention right."

68. A "public authority" would plainly include the Secretary of State, the intelligence and security agencies and the police. It would also include the IPC and, as subsection (3)(a) makes clear on the express words of the HRA, it includes a court or tribunal. Accordingly, the IPT is subject to the obligation in section 6(1) of the HRA as are the other public authorities concerned.

69. There is an exception made by subsection (2) to the obligation in subsection (1), so far as material, if:

> "(a) as the result of one or more provisions of primary legislation, the authority could not have acted differently …"

70. This has the consequence that, where a public authority has a discretion to act under primary legislation (and is therefore not required to act in a particular way) it must exercise its discretion in a way which is compatible with the Convention rights. In such circumstances it would not be open to the authority to say that it "could not" have acted differently as a result of primary legislation.

71. Furthermore, section 6(2) needs to be read together with the strong obligation of interpretation in section 3(1) of the Act, which requires that:

> "So far as it is possible to do so, primary legislation … must be read and given effect in a way which is compatible with the Convention rights."

72. It is only in circumstances where primary legislation cannot, even in accordance with the strong obligation in section 3, be read and given effect in a way which is compatible with the Convention rights that the provisions of section 4 of the HRA become relevant.

73. Section 4, so far as material, provides that if a relevant court is satisfied that the provision is incompatible with a Convention right, "it may make a declaration of that incompatibility": see subsection (2). The relevant courts listed in subsection (5) include (in England and Wales) the High Court.

74. Subsection (6) is important because it makes it clear that:

> "A declaration under this section ('a declaration of incompatibility') –
>
> (a) does not affect the validity, continuing operation or enforcement of the provision in respect of which it is given; and
>
> (b) is not binding on the parties to the proceedings in which it is made."

75. What the making of a declaration of incompatibility does do is to enable a Minister of the Crown to make a "remedial order" where the provisions of section 10 of the HRA are satisfied. In effect this enables the government to amend primary legislation so as to remove an incompatibility with the Convention rights by means of secondary legislation. Sch. 2 to the HRA makes further provision about remedial orders.

Caselaw of the European Court of Human Rights on "in accordance with the law"

76. As is plain from the wording of Article 8(2) of the ECHR, any interference with the rights in Article 8(1) must be in accordance with the law. There is a similar provision in Article 10(2), which refers to an interference having to be "prescribed by law". The caselaw of the European Court of Human Rights has made it clear for many years that this requirement has three elements:

(1) The interference must be authorised by domestic law. This is a necessary condition for compatibility with the Convention but it is not a sufficient condition.

(2) The domestic law must have a certain "quality". In particular it must be accessible.

(3) The quality of law also entails that it must be reasonably foreseeable.

77. In *Weber and Saravia v Germany* (2008) 46 EHRR SE5 the Court (Third Section) summarised the requirement of foreseeability in the context of secret measures of surveillance, such as telephone intercepts, in the following way:

> "93. As to the third requirement, the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly … However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident … It is therefore essential to have 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 in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures …
>
> 94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise

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

78. It is well established in the case law on the Convention, and was common ground before us, that the requirement that safeguards must be set out in statute law in fact can be satisfied by provisions which are in a document such as a code of practice issued under statute: see e.g. *Silver v UK* (1983) 5 EHRR 347, at para. 89. For that reason, the scheme with which this Court is concerned in the present case, and which is summarised in the overview set out in the Annex to this judgment, includes relevant provisions of the codes of practice made under the IPA as well as the Act itself.

79. Turning to the question of whether an interference is "necessary in a democratic society", in *Weber and Saravia*, at para. 106, the Court said:

> "The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a *fairly wide* margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security … Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse … This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law …" (emphasis added)

80. In *Zakharov v Russia* (2016) 63 EHRR 17, the Grand Chamber of the European Court of Human Rights in large part reiterated those general principles at paras. 227-234 of its judgment. However, as Mr Martin Chamberlain QC pointed out at the hearing before us, at para. 232, the Court referred to the margin of appreciation enjoyed by a national authority in this context as being "a *certain* margin of appreciation in

choosing the means for achieving the legitimate aim of protecting national security." (emphasis added)

81. At paras. 233-234, the Court said:

> "233. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in supervisory procedures if the bounds of necessity, within the meaning of Article 8(2), are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.
>
> 234. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications."

82. That last proposition was the subject of footnote 205 in the judgment, which cross-refers to the Court's earlier judgment in *Kennedy v UK* (2011) 52 EHRR 4, at paras. 155 and 167.

Guidance from the Supreme Court on "in accordance with the law"

83. Valuable guidance was recently given by the Supreme Court as to the distinction between the requirement that an interference with human rights must be "in accordance with the law" and the requirement that such an interference must be

"necessary in a democratic society", in particular so as to comply with the principle of proportionality. In *R (P) v Secretary of State for Justice* [2019] UKSC 3; [2019] 2 WLR 509 the main judgment was given by Lord Sumption (with whom Lord Carnwath JSC and Lord Hughes agreed). Lord Sumption discussed the issue of the requirement that an interference must be "in accordance with the law" at paras. 14-41. Having referred in detail to the authorities both from the European Court of Human Rights and domestic courts, Lord Sumption concluded, at para. 41, that the reference in the caselaw to the need for safeguards against "arbitrary" interference with Convention rights, when firmly placed in its proper context, is a reference "to safeguards essential to the rule of law because they protect against the abuse of imprecise rules or unfettered discretionary powers."

84. Earlier, at para. 31, Lord Sumption referred in particular to the present sort of context and said:

> "… An excessively broad discretion in the application of a measure infringing the right of privacy is likely to amount to an exercise of power unconstrained by law. It cannot therefore be in accordance with law unless there are sufficient safeguards, exercised on known legal principles, against the arbitrary exercise of that discretion, so as to make its application reasonably foreseeable."

85. Earlier in his judgment Lord Sumption made it clear that the requirement of "law" is a binary one: see para. 14. It is not a question of degree. A measure either has the quality of law or it does not. "This is because it relates to the characteristics of the legislation itself, and not just to its application in any particular case: see *Kruslin v France* (1990) 12 EHRR 547, paras. 31-32." This is in contrast to the question of proportionality, which is a question of degree: see para. 17.

86. At para. 17, Lord Sumption said:

> "… A measure is not 'in accordance with the law' if it purports to authorise an exercise of power unconstrained by law. The measure must not therefore confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself. Nor should it be couched in terms so vague or so general as to produce substantially the same effect in practice. The breadth of a measure and the absence of safeguards for the rights of individuals are relevant to its quality as law where the measure confers discretion, in terms or in practice, which make its effects insufficiently foreseeable. Thus a power whose exercise is dependent on the judgment of an official as to when, in what circumstances or against whom to apply it, must be sufficiently constrained by some legal rule governing the principles on which that decision is to be made. But a legal rule imposing a duty to take some action in every case to which the rule applies does not necessarily give rise to the same problem. It may give rise to a different problem when it comes to necessity and proportionality, but that is another issue. If the question is how much discretion is too much, the only legal tool

> available for resolving it is a proportionality test which, unlike the test of legality, is a question of degree."

The importance of the nature of the alleged incompatibility

87. There can be instances where legislation is in accordance with the concept of "law" in the Convention sense but is incompatible with the principle of proportionality. The complaint in such a case is not about the application of the legislation to the facts of a particular case but to the terms of the legislation itself. A well known example of this is to be found in section 3 of the Representation of the People Act 1983, which has been the subject of much litigation both in Strasbourg and in the domestic courts. That provision is both short and clear. It makes it clear that no person who is convicted of a criminal offence may vote in elections while he is a serving prisoner. The issue in cases such as *Hirst v United Kingdom (No. 2)* (2006) 42 EHRR 41 and *R (Chester) v Secretary of State for Justice* [2013] UKSC 63; [2014] AC 271 was not whether the legislation was in accordance with the concept of "law": it plainly was. Nor was it a question of whether the legislation could be applied to the facts of a particular case in accordance with the principle of proportionality. The complaint was that the legislation itself was incompatible with that principle because it imposed a blanket ban on all serving prisoners.

88. It will be seen therefore that in principle an application can be made for a declaration of incompatibility of primary legislation where the nature of the allegation is that it is the legislation itself which is incompatible with the Convention rights. This is in substance a kind of constitutional review of primary legislation, so as to assess its compatibility with fundamental human rights, even though there is an important limit on the courts' power to grant a remedy. As we have indicated earlier, the scheme of the HRA is such that the higher courts have the power to declare primary legislation to be incompatible with the Convention rights but they have no power to strike it down or disapply it. The legislation continues to have effect unless and until it is amended or repealed. A declaration of incompatibility is not binding on the parties, let alone on Parliament. Although a declaration of incompatibility may have political or moral effect, the only legal effect of such a declaration is that it enables the government to amend the incompatible primary legislation by way of secondary legislation, described in the HRA as a "remedial order", under section 10. The government has a discretion as to whether it wishes to use that route to cure the incompatibility. Sometimes that route has been taken, as after a case concerning the Mental Health Act 1983: *R (H) v Mental Health Review Tribunal for North and East London Region* [2001] EWCA Civ 415; [2002] QB 1. More often in practice it has been Parliament itself which has enacted primary legislation to remove the incompatibility which has been declared to exist by a court, as happened in the case of Part 4 of the Anti-terrorism, Crime and Security Act 2001 after *A v Secretary of State for the Home Department* [2004] UKHL 56; [2005] 2 AC 68.

89. It is important to appreciate, however, that such cases where primary legislation itself is intrinsically incompatible with those rights will be relatively rare. More often primary legislation will not itself be intrinsically incompatible with the Convention rights: its application to a particular case may be in breach of the Convention rights, depending on the concrete facts. But that would not be a case where it would be

appropriate or even possible to grant a declaration of incompatibility. It would be a more conventional case, in which it is argued (and may be found by a court) that the act of the executive (for example one of the intelligence agencies) is in breach of section 6 of the HRA.

90. Furthermore, it should always be recalled that all legislation, including primary legislation, must (so far as possible) be read and given effect in a way which is compatible with the Convention rights: section 3 of the HRA. It is well established that the obligation of interpretation in section 3 is a strong one and may require an interpretation which is not the natural interpretation of legislation and may lead, for example, to the reading of words into legislation so as to render it compatible with the Convention rights: see *Ghaidan v Godin-Mendoza* [2004] UKHL 30; [2004] 2 AC 557. Nevertheless, there is a line which must not be crossed between interpretation and legislation. The court has no power under section 3 to engage in judicial legislation: see *In re S (Minors) (Care Orders: Implementation of Care Plans)* [2002] UKHL 10; [2002] AC 291.

Use of Hansard in cases concerning the compatibility of primary legislation under the HRA

91. Cases such as this one, in which the court is required to assess the compatibility of primary legislation with Convention rights, potentially raise a point of constitutional importance: to what extent can the courts properly refer to statements made in Parliament? This was considered by the House of Lords in *Wilson v First County Trust Ltd (No 2)* [2003] UKHL 40; [2004] 1 AC 816, in particular at paras. 51-67 in the opinion of Lord Nicholls of Birkenhead. Although this country does not have a written constitution, it certainly does have constitutional principles. One of those constitutional principles is the separation of powers, in particular as between Parliament and the courts. As Lord Nicholls put it at para. 55:

> "… The courts and Parliament are both astute to recognise their constitutional roles … These distinct roles reflect one aspect of the separation of powers under this country's constitution."

A particular manifestation of that wider constitutional principle is Article 9 of the Bill of Rights 1689, which provides, in modern spelling, that:

> "The freedom of speech and debates or proceedings in Parliament ought not to be impeached or questioned in any court or place out of Parliament."

92. As Lord Nicholls further observed, at para. 61, the HRA requires the courts to exercise a new role in respect of primary legislation:

> "… This new role is fundamentally different from interpreting and applying legislation. The courts are now required to evaluate the effect of primary legislation in terms of Convention rights and, where appropriate, make a formal declaration of incompatibility. In carrying

> out this evaluation the court has to compare the effect of the legislation with the Convention right. If the legislation impinges upon a Convention right the court must then compare the policy objective of the legislation with the policy objective which under the Convention may justify a prima facie infringement of the Convention right. When making these two comparisons the court will look primarily at the legislation, but not exclusively so. Convention rights are concerned with practicalities. When identifying the practical effect of an impugned statutory provision the court may need to look outside the statute in order to see the complete picture … As to the objective of the statute, at one level this will be coincident with its effect. … But that is not the relevant level for Convention purposes. What is relevant is the underlying social purpose sought to be achieved by the statutory provision. Frequently that purpose will be self-evident, but this will not always be so."

93. At para. 62 Lord Nicholls observed that the legislation must not only have a legitimate policy objective. It must also satisfy the test of proportionality.

> "The court must decide whether the means employed by the statute to achieve the policy objective is appropriate and not disproportionate in its adverse effect. This involves a 'value judgment' by the court, made by reference to the circumstances prevailing when the issue has to be decided. …"

94. At para. 63 Lord Nicholls said that, when a court makes this value judgment, the facts

> "will often speak for themselves. But sometimes the court may need additional background information tending to show, for instance, the likely practical impact of the statutory measure and why the course adopted by the legislature is or is not appropriate. Moreover, as when interpreting a statute, so when identifying the policy objective of a statutory provision or assessing the 'proportionality' of a statutory provision, the court may need enlightenment on the nature and extent of the social problem (the 'mischief') at which the legislation is aimed. This may throw light on the rationale underlying the legislation."

95. At para. 64 Lord Nicholls said that this additional background material may be found in published documents such as a government white paper. It could also in principle include statements made by a minister or another member of either House in Parliament. He said that the courts must be able to take this into account and would be failing in their duty to discharge the new role assigned to them by Parliament in the HRA if they were to exclude from their consideration relevant background information whose only source was a ministerial statement in Parliament. By having

regard to such material the court would not be "questioning" proceedings in Parliament or intruding improperly into the legislative process:

> "The court would merely be placing itself in a better position to understand the legislation."

96. At para. 65 Lord Nicholls said that:

> "it is difficult to see how there could be any objection to the court taking account of something said in Parliament when there is no suggestion the statement was inspired by improper motives or was untrue or misleading and there is no question of legal liability."

97. Finally, at para. 67, Lord Nicholls said that, beyond this use of Hansard as a source of background information,

> "the content of parliamentary debates has no direct relevance to the issues the court is called upon to decide in compatibility cases and, hence, these debates are not a proper matter for investigation or consideration by the courts."

He continued:

> "In particular, it is a cardinal constitutional principle that the will of Parliament is expressed in the language used by it in its enactments. The proportionality of legislation is to be judged on that basis. The courts are to have due regard to the legislation as an expression of the will of Parliament. The proportionality of a statutory measure is not to be judged by the quality of the reasons advanced in support of it in the course of parliamentary debate, or by the subjective state of mind of individual ministers or other members. … Lack of cogent justification in the course of parliamentary debate is not a matter which 'counts against' the legislation on issues of proportionality. The court is called upon to evaluate the proportionality of the legislation, not the adequacy of the minister's exploration of the policy options or of his explanations to Parliament. The latter would contravene article 9 of the Bill of Rights. The court would then be presuming to evaluate the sufficiency of the legislative process leading up to the enactment of the statute. …"

98. Against that important background of principle, we confess that we did not find helpful the Defendants' citation of certain passages from Hansard as the Investigatory Powers Bill was proceeding through Parliament. We consider that Mr Ben Jaffey QC was right to submit that it put the Claimant in the invidious position of having to suggest that statements made by ministers in Parliament were wrong. In our view, the

invitation to rely on those statements came perilously close (to put it no higher) to requiring this Court to assess the quality of the reasoning given by ministers for what became the 2016 Act. As Lord Nicholls made it clear in *Wilson*, that is not the proper function of the court when considering the compatibility of primary legislation with the Convention rights. Fortunately, we have not found it necessary to have regard to Hansard in order to adjudicate fairly on the issues before this Court.

The jurisdiction of the Investigatory Powers Tribunal

99. During the course of the hearing before us it became apparent that there is an important issue which divides the parties as to the circumstances in which the IPT may entertain a complaint about secret surveillance.

100. On behalf of the Claimant Mr Chamberlain emphasised that in this country, and in contrast to some other European states, individuals are not given any notification that they have been the subject of surveillance by the intelligence and security agencies. This is reflected in the well established practice that those agencies will "neither confirm nor deny" that a person has been the subject of surveillance (a practice known as "NCND").

101. The Claimant submits that, without any general notification requirement, the ability to seek a remedy before the IPT is "a weak safeguard": see para. 116 of the Re-amended Statement of Facts and Grounds for judicial review. The Defendants dispute this: see para. 111 of their Detailed Grounds of Resistance.

102. The jurisdiction of the IPT was considered by the European Court of Human Rights in *Kennedy v United Kingdom* (2011) 52 EHRR 4. At paras. 75-76 the Court noted that the IPT was established under section 65(1) of RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by RIPA. Any person may bring a claim before the IPT and, save for vexatious or frivolous applications, the IPT must determine all claims brought before it: see section 67(1), (4) and (5).

103. Further, section 65(2) of RIPA provides that the IPT is the *only* appropriate forum in relation to proceedings for acts incompatible with Convention rights which are brought against any of the intelligence services; and complaints by persons who allege to have been subject to the investigatory powers of RIPA.

104. At para. 167 of its judgment the Court highlighted

> "the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. …"

105. At para. 183 of its judgment the Court recorded that the Government argued in that case that the procedure before the IPT offered as fair a procedure as could be achieved in the context of secret surveillance powers:

> "In particular, a complainant did not have to overcome any evidential burden to apply to the IPT and any legal issues could be determined in a public judgment after an inter partes hearing. Further, the IPT had full powers to obtain any material it considered necessary from relevant bodies and could call upon the assistance of the Commissioner [the predecessor to the IPC]. It could appoint an advocate to assist it at closed hearings. Finally, in the event that the complainant was successful, a reasoned decision would be provided. …"

106. That submission as to the absence of any evidential burden was accepted by the Court: see para. 190 of its judgment.

107. The Claimant now submits that the IPT has altered its approach on standing in the case of *Human Rights Watch Inc and Ors v Secretary of State for Foreign and Commonwealth Affairs and Ors* [2016] UKIPTrib 15 165-CH, in which the judgment of a five member panel was delivered by Burton J (the then President of the IPT).

108. The *Human Rights Watch* case followed a campaign by Privacy International to encourage people to make claims in the IPT in standard form following a case in which it had been successful: 663 claims were then made. In the *Human Rights Watch* case the IPT restated its commitment to the efficient disposal of claims brought by persons with grounds of some kind for believing that their communications have been intercepted, as opposed to being a recipient of possibly hundreds or thousands of applications from people who have no such basis other than the mere existence of the legislation: see para. 44 of the IPT judgment. The IPT found that some of the claims before it should be considered because the claimants did have standing. Others were rejected.

109. At para. 46 Burton J said:

> "We are satisfied that the appropriate test for us to operate, which would accord with *Zakharov* and our obligations under RIPA, is whether in respect of the asserted belief that any conduct falling within subsection s.68(5) of RIPA has been carried out by or on behalf of any of the Intelligence Services, there is any basis for such belief; such that the 'individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures.' (*Zakharov* at 171). *This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated.*" (Emphasis added)

110. The reference is to *Zakharov v Russia*, a decision of the Grand Chamber of the European Court of Human Rights, which we have already cited above. In that case, at para. 171, after referring back to its earlier decision in *Kennedy*, the Court said that, where the domestic system does not afford an effective remedy to a person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused "cannot be said to be unjustified." In such circumstances the individual does not need to demonstrate the existence of any risk that secret surveillance measures were in fact applied to him or her:

> "By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures."

111. In these proceedings the Claimant submits that, in the light of what is said to be a change of approach by the IPT, the First Section of the European Court of Human Rights misunderstood the current position in its judgment in *Big Brother Watch*, in particular at para. 379.

112. We cannot see any inconsistency in the approach which the IPT has taken at all material times, as is made plain by its judgment in the *Human Rights Watch* case, in particular at para. 46. In that passage the IPT clearly considered both that it was continuing (not changing) its traditional practice and that its practice was consistent with the judgment in *Zakharov*. We respectfully agree.

The decision of the First Section in *Big Brother Watch*

113. Before we turn to address the Claimant's grounds of challenge in more detail, it is important that we should summarise here the recent decision of the First Section of the European Court of Human Rights in *Big Brother Watch*. In that case the applicants raised complaints about the compatibility with Article 8 of three discrete regimes, two of which are relevant for present purposes. The first was the regime for the bulk interception of communications under section 8(4) of RIPA; the second was the regime for the acquisition of communications data under Part 1, Chapter II of RIPA.

114. The Court began its consideration of the section 8(4) regime at para. 270 of its judgment. At paras. 303-310 the Court set out the general principles relating to secret measures of surveillance, including the interception of communications, by reference to its earlier caselaw, including *Weber and Saravia* and *Zakharov*.

115. At para. 306 the Court said:

> "… The law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference …"

116. The Court observed that it had previously developed the six minimum requirements that should be set out in law in order to avoid abuses of power (we have already summarised these by reference to *Weber and Saravia*). The Court also observed in the same paragraph that in *Zakharov* it had confirmed that the same six minimum requirements applied in cases where the interception was for reasons of national security. However, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

117. At paras. 309-310 the Court repeated what it had said in *Zakharov* about the three stages at which review and supervision of secret surveillance may come into play.

118. At paras. 311-313 the Court considered its existing caselaw on the bulk interception of communications. It noted that it had previously considered the issue on two occasions: first in *Weber and Saravia* and then in *Liberty and Others v UK* (Application No 58243/00, judgment of 1 July 2008).

119. In *Weber and Saravia* the Court had held the complaint under Article 8 to be manifestly ill-founded, having particular regard to the six minimum requirements. The Court considered that there did exist adequate and effective guarantees against abuses of the state's strategic monitoring powers.

120. In the *Liberty* case, the Court considered the regime under section 3(2) of the Interception of Communications Act 1985, which was in effect the predecessor of the regime under section 8(4) of RIPA. It allowed the executive to intercept communications passing between the UK and an external receiver. It provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered that this was required in the interests of national security, the prevention of serious crime or the protection of the UK's economy. The Court held that the domestic law at the relevant time (which pre-dated the adoption of the Interception of Communications Code of Practice, to which the Court referred at para. 109 of its judgment) did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the state to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.

121. At paras. 314-320 of *Big Brother Watch* the Court addressed the test to be applied in the case before it.

122. At para. 314 of *Big Brother Watch* the Court observed that it had accepted in *Weber and Saravia* and *Liberty* that bulk interception regimes did not *per se* fall outside the

"wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security". Although those cases were now more than 10 years old, given developments since then, including the scourge of global terrorism, the Court considered that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within states' margin of appreciation.

123. Nevertheless, at para. 315, the Court said that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation. Therefore, while states enjoy a wide margin of appreciation in deciding what type of interception and regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower. In this regard the Court had identified six minimum requirements that both bulk interception and other interception regimes must satisfy in order to be sufficiently foreseeable to minimise the risk of abuses of power.

124. The Court noted, at para. 316, that the applicants argued that the Court should "update" those requirements by including requirements for objective evidence of reasonable suspicion in relation to the persons for whom data is being sought, prior independent judicial authorisation of interception warrants, and subsequent notification of the surveillance subject. The Court rejected that invitation. It said, at para. 316:

> "… while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasised this point in its caselaw, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In any event, although the Court would agree that the additional requirements proposed by the applicants might constitute important safeguards in some case, for the reasons set out below it does not consider it appropriate to add them to the list of minimum requirements in the case at hand."

125. The first of those reasons was set out at para. 317:

> "… Requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgement that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. Bulk interception is by definition untargeted, and to require 'reasonable suspicion' would render the operation of such a scheme impossible. Similarly, the requirement of 'subsequent notification' assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime."

126. The Court then turned to the possible imposition of a requirement for judicial authorisation. At para. 318 it said that this was not inherently incompatible with the effective functioning of bulk interception but that, as the Venice Commission had acknowledged in its report on the democratic oversight of signal intelligence agencies (referred to at para. 212 of the judgment), while the Court has recognised that judicial authorisation is an "important safeguard against arbitrariness", to date it has not recognised it to be a "necessary requirement". The Court noted in this context that there would appear to be good reason for this. It had found it to be desirable to entrust supervisory jurisdiction to a judge because, as a result of the secret nature of the surveillance, the individual would usually be unable to seek a remedy of his or her own accord. However, the Court noted that this was not the case in every contracting State: for example, in the UK, any person who thinks that he or she has been subject to secret surveillance can lodge a complaint to the IPT. Consequently, in *Kennedy* the Court had accepted that, regardless of the absence of prior judicial authorisation, the existence of independent oversight by the IPT and the then Interception of Communications Commissioner did provide adequate safeguards against abuse: see *Kennedy*, at paras. 167-169. We have already referred to this topic earlier in our judgment.

127. At para. 320, the Court said that, while it considered judicial authorisation to be an important safeguard and perhaps even "best practice", by itself it can neither be necessary nor sufficient to ensure compliance with Article 8:

> "Rather, regard must be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse …"

The Court therefore proceeded to examine the justification for any interference before it by reference to the six minimum requirements and it also had regard to the additional relevant factors which it had identified in *Zakharov* but did not classify as minimum requirements (see our consideration of *Zakharov* above).

128. At para. 328 of its judgment the Court turned to the first two minimum requirements in *Weber and Saravia*, which are the nature of the offences which might give rise to an interception order; and a definition of the categories of people liable to have their telephones tapped. The Court referred to these together as relating to "the scope of application of secret surveillance measures".

129. At para. 329 the Court set out what it understood to be the four distinct stages of the section 8(4) regime:

(1) The interception of a small percentage of internet "bearers", selected as being those most likely to carry external communications of intelligence value. Bearers are in effect communications links in an electronic "pipeline" which enable traffic to flow through the internet.

(2) The filtering and automatic discarding (in near real-time) of a significant percentage of intercepted communications, being the traffic least likely to be of intelligence value.

(3) The application of simple and complex search criteria (by computer) to the remaining communications, with those that match the relevant "selectors" being retained and those that do not being discarded.

(4) The examination of some (if not all) of the retained material by an analyst.

130. The Court then considered the four stages by reference to the first two minimum requirements in some detail.

131. At para. 337 the Court said that:

> "… While anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish. … "

132. At para. 338 the Court said, by reference to what the ISC had suggested, that "it would be desirable for the criteria for selecting the bearers to be subject to greater oversight by the Commissioner …" However, the Court had already noted that by its very nature a bulk interception regime will allow the authorities a broad discretion to intercept communications, and, as such,

> "it does not consider this fact alone to be fatal to the Article 8 compliance of the section 8(4) regime. While the discretion to intercept should not be unfettered … more rigorous safeguards will be required at the third and fourth stages identified in paragraph 329 above, as any interference in such cases will be significantly greater."

133. The Court then turned to the selectors and search criteria used. At para. 340 it said that these do not need to be made public nor do they necessarily need to be listed in the warrant ordering interception. The Court noted that in the *Liberty* proceedings the IPT had found that the inclusion of the selectors in the warrant or accompanying certificate would "unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic". The Court had no reason to call that conclusion into question. It continued:

> "… Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight; a safeguard which appears to be absent in the section 8(4) regime. …"

134. At para. 342 the Court noted that the Independent Reviewer of Terrorism Legislation had recommended that the purposes for which material or data was sought should be spelled out by reference to specific operations or missions. In order for this safeguard to be effective, the Court agreed that it would be highly desirable for the certificate to

be expressed in more specific terms than it currently appeared to be. We would respectfully note that the 2016 Act has introduced the concept of "operational purposes", although Mr Jaffey criticised that as being in substance no different from the concept of a certificate under section 15 of RIPA.

135. Mr Jaffey placed some emphasis on para. 343 of the judgment:

> "… On the other hand, the exclusion of communications of individuals known currently to be in the British Islands is, in the opinion of the Court, an important safeguard, since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA. The intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant."

136. At para. 345 the Court said:

> "On balance, the Court agrees that it would be preferable for the selection of material by analysts to be subject at the very least to pre-authorisation by a senior operational manager. However, given that analysts are carefully trained and vetted, records are kept and those records are subject to independent oversight and audit …, the absence of pre-authorisation would not, in and of itself, amount to a failure to provide adequate safeguards against abuse."

137. Nevertheless, at para. 346, the Court said that it had to have regard to the operation of the section 8(4) regime as a whole, and in particular the fact that the list from which analysts select material is itself generated by the application of selectors and selection criteria which are not subject to any independent oversight. Having considered *Kennedy* and *Liberty*, the Court said that:

> "… In a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable to the filtering and selecting for examination stage must necessarily be more robust."

138. The Court concluded this section of its judgment at para. 347 as follows:

> "Therefore, while there is no evidence to suggest that the intelligence services are abusing their powers … the Court is not persuaded that the safeguards governing the selection of bearers for interception and selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of

> the selectors and search criteria used to filter intercepted communications."

139. In the light of the judgment of the First Section the Defendants wrote to the IPC a letter dated 10 December 2018, in which they set out the steps that they proposed to take to address the violations of the Convention which had been found by the European Court of Human Rights to the limited extent that they had been. The first violation concerning oversight of selectors was addressed in the following way:

> "The first violation identified by the Court, summarised at paragraph 347 of the judgment, relates to concerns that there should be more robust independent oversight of the selectors (search terms) that are used by analysts to examine material that has been collected under a bulk interception warrant. This finding, of course, relates to the previous regime and the IP Act has now introduced significantly heightened safeguards relating to the selection for examination of data collected under any bulk warrant. These additional safeguards include the introduction of operational purposes, which limit the purposes for which bulk data may be examined. Those purposes must be set out on every bulk warrant so that it is foreseeable to the Secretary of State, and Judicial Commissioner, how the data collected under the warrant may be used. In addition, the Act introduces new criminal offences for the breach of examination safeguards, which will act as a strong deterrent to prevent abuse of bulk powers. In relation to the oversight of selectors specifically, this now sits within scope of your main oversight functions in the IP Act: as part of the requirement that you keep under review the exercise by public authorities of statutory functions relating to the interception of communications. Furthermore, the investigation and information powers that you have been granted under the IP Act enable you to require the provision of any information from public authorities that you may require in exercising your functions, including in relation to selectors.
>
> These factors, taken together, respond substantively to this violation. Nevertheless, in order to assist your oversight in this area our officials and those from the intelligence services, GCHQ in particular, have committed to work with your office to establish how the oversight of selectors could be enhanced and how this would be best taken forward in practice."

140. In our view, what is important in the present context is to recall that the 2016 Act has created a new system of supervision through the office of the IPC. There is nothing in the judgment in *Big Brother Watch* which requires there to be prior judicial or independent authorisation of bearers or selectors and search criteria. To the contrary, the Court rejected the submission that there should be judicial authorisation. What it

does require is sufficiently robust independent oversight. In our view, that is now provided by the office of the IPC.

141. Against the above background of principle we now turn to address each of the Claimant's main grounds of challenge.

The challenge to the regime for bulk interception warrants

142. Bulk interception warrants are governed by Chapter 1 of Part 6 of the 2016 Act. A more detailed summary of the statutory provisions can be found in the overview in the Annex to this judgment, at paras. 12-16; and 25-45.

143. As is apparent from that overview, a bulk interception warrant must have "the main purpose" of either the interception of "overseas-related" communications or the obtaining of "secondary data" from such communications: see section 136(2).

144. The warrant may only be issued by the Secretary of State personally. The criteria of which the Secretary of State must be satisfied are outlined in the overview at para. 26.

145. The warrant must also specify the operational purposes for which any material obtained under it may be selected for examination. Those operational purposes are the subject of specific statutory provision, for example in section 142 of the 2016 Act: see para. 34 of the overview.

146. The warrant must satisfy the requirements of necessity and proportionality: see para. 31 of the overview.

147. The Secretary of State must be satisfied that there are safeguards in place in respect of matters such as retention, copying and disclosure: see paras. 36-41 of the overview.

148. Importantly, in our view, the Act requires the Secretary of State to "ensure" that safeguards relating to the examination of material are in force before issuing a bulk interception warrant: see para. 42 of the overview. At the hearing before us Sir James Eadie accepted on behalf of the Defendants that this was a justiciable legal duty. That means that the Secretary of State is not only politically accountable, to Parliament, but also accountable (in principle) to relevant courts and tribunals for the fulfilment of that statutory duty.

149. Very importantly, in our view, the warrant must also be authorised by a JC. As we have already seen JCs must be persons who hold or have held a high judicial office, in other words at least a High Court Judge. The IPC himself is currently a serving Lord Justice of Appeal.

150. The requirement for approval of a warrant by a JC is part of the so called "double lock" system which the 2016 Act introduced. There was no such system under previous legislation such as RIPA, which was the subject of the judgment of the First Section in *Big Brother Watch*.

151. Furthermore, as is apparent from the overview at paras. 109-120, the JCs have a number of other important functions, including oversight by way of audit, inspection

and investigation. In our view, these are important safeguards which have been introduced by the 2016 Act. They are to be seen as part of the overall, inter-locking structure which the Act has created.

152. We would make two further preliminary observations about the scheme of the 2016 Act.

153. First, it is common ground for present purposes that the mere fact that a statute confers powers to obtain information in bulk does not render it incompatible with the Convention rights. That concession is made on the basis of the judgment of the First Section in *Big Brother Watch* and the Claimant reserves its position depending on what the Grand Chamber may say in that case in due course. Nevertheless, that is the legal background against which this Court must decide the issues before it now.

154. Secondly, as we have already indicated, what is sought from this Court in these proceedings is a declaration of incompatibility in respect of the 2016 Act. The essential focus of the Claimant's submissions has been on the requirement that the Act must be "in accordance with the law" within the Convention meaning of that concept.

155. Although at times the Claimant also submits that the Act is in breach of the principle of proportionality and therefore not "necessary in a democratic society", it seems to us that that submission will be better directed at any particular application of the Act. This is not a case (such as those concerning prisoner voting) in which it can be said that a provision in primary legislation is intrinsically incompatible with the Convention rights. Whether or not there is a breach of the Convention rights will often turn on a close consideration of the application of the Act to the facts of a particular case.

156. What in essence the Claimant submits is that the 2016 Act does not contain sufficient safeguards against the risk of abuse of discretionary powers, with the consequence that the Act itself is incapable of applying in a way which is compatible with Convention rights. We do not accept that broad submission. We consider that the inter-locking provisions of the Act do contain sufficient safeguards against the risk of abuse of discretionary powers.

157. In essence we accept the submissions which were made by Sir James Eadie on behalf of the Defendants and are not persuaded that the 2016 Act is incompatible with the Convention rights insofar as the challenge concerns the bulk interception powers regime.

158. The starting point is to note the important reality that the ability to effect interception in bulk is a critical capability for the intelligence services so as to protect the public. This is evidenced before the Court in the first witness statement of Mr Dix, at para. 190. The reason for its utility is that, at this early stage, it may simply be impossible to know who may turn out to be a subject of interest. Searches for traces of activity by individuals can take place who are not yet known and patterns of activity might be identified which indicate a threat to the UK.

159. We note in this context that, in his Bulk Powers Review (August 2016), Lord Anderson said that there was a proven operational case for this power, which had

shown itself to be of "vital utility" in various operational contexts, both in relation to "target discovery" and "target development, the triaging of leads and as a basis for disruptive action". Lord Anderson also considered that various suggested alternatives to bulk interception "fall short of matching the results that can be achieved using the bulk interception capability" and "may also be slower, more expensive more intrusive or riskier to life": see para. 190 of the first witness statement of Mr Dix; and the original report at para. 5.54.

160. Secondly, we accept the fundamental submission made on behalf of the Defendants that the question of compatibility with the Convention must be determined by reference to the totality of the inter-locking safeguards applicable at the various stages of the bulk interception process. In particular it must not be done by reference to the potential breadth of the information that could in principle be retained under the bulk interception power. That latter question may be relevant in any assessment of proportionality which has to be done but it does not render the 2016 Act itself incompatible with the Convention rights by reason of the requirement that it must be in accordance with the law.

161. Thirdly, arising from that point, we accept the submission that it is simply not possible to transpose findings made by the First Section in *Big Brother Watch* across to the new statutory scheme in the 2016 Act. In particular, it seems to us that the Claimant has significantly played down the importance of the introduction of the office of the IPC which is created by the 2016 Act. For example, the need for the "double lock", including approval by a Judicial Commissioner at the warrant stage before bulk data can even be obtained is one of the key features of the new regime in the 2016 Act.

162. Fourthly, we accept that there will be an ability to regulate the selection of bearers since there is a requirement that the warrant application must contain a description of the communications to be intercepted: see section 136 of the IPA and the Interception Code of Practice, para. 6.20(b).

163. The selection of bearers is also subject to the provisions of para. 6.10 of the Interception Code, which requires the intelligence services to select them for interception on the basis of regular surveys of those bearers most likely to contain overseas-related communications, relevant to the operational purposes specified in the warrant.

164. Fifthly, we note that the 2016 Act has narrowed the definition of "overseas-related communication" as compared with the meaning of "external communication" in section 20 of RIPA. The definition of external communication in RIPA was "a communication sent or received outside the British Islands". In contrast, section 136(3) of the 2016 Act defines "overseas-related communication" to mean "(a) communications sent by individuals who are outside the British Islands, or (b) communications received by individuals who are outside the British Islands." The reason why this is a narrower definition was explained in the proceedings brought by Liberty before the IPT: *Liberty and Ors v GCHQ & Ors* [2014] UKIPTrib 13_77-H; [2015] HRLR 2. In that case evidence was given on behalf of the Government by a witness called Charles Farr. He explained that, under RIPA, "external communications" would include a communication between a person and thing (for example a server located outside the UK): therefore if a person in the British Islands

undertook a Google search, that was an external communication for the purposes of of Chapter I of Part 1 of RIPA. It will no longer be possible, according to the definition in section 136(3) of the 2016 Act, to regard Google searches by persons within the British Islands as "overseas-related communications".

165. Sixthly, we are not persuaded that the fact that only the "main" purpose of a bulk interception warrant has to be the interception of an overseas-related communications or the obtaining of secondary data therefrom renders this incompatible with the Convention rights. There is nothing in Convention authority to that effect. Further, para. 6.9 of the Interception Code states that a bulk warrant authorises the interception of communications that are not overseas-related "to the extent that it is necessary in order to intercept the overseas-related communications to which the warrant relates". This and other matters relating to necessity and proportionality will be amongst those which can be considered both by the Secretary of State and the JC when they are asked to approve the grant of a bulk interception warrant.

166. Seventhly, we agree with the Secretary of State's submission that the requirement of "operational purposes" is a safeguard which is relevant to the selection of bearers. In that context we turn in more detail to the provisions of section 142 of the 2016 Act.

167. Section 142(3) requires that a bulk interception warrant must specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination. Subsection (4) provides that the operational purposes specified in the warrant must be ones specified, in a list maintained by the heads of the intelligence services, as purposes which they consider are operational purposes for which intercepted content or secondary data obtained under bulk interception warrants may be selected for examination. The list of operational purposes must be approved by the Secretary of State: see subsection (6). The Secretary of State may give such approval only if satisfied that the operational purpose is specified in a greater level of detail than the descriptions contained in section 138(1)(b) or (2): see subsection (7). At the end of each relevant three-month period the Secretary of State must give a copy of the list of operational purposes to the Parliamentary ISC: see subsection (8). Finally, the Prime Minister must review the list of operational purposes at least once a year: see subsection (10). These are not to be belittled as insignificant safeguards, as they build together an intricate set of modes of accountability, which involve Parliament as well as members of the government at the highest level.

168. Furthermore, the same considerations, including the requirement of operational purposes, will be a constraint on selectors and search criteria for examination.

169. It is important not to overlook the powers given to the IPC, in particular under section 229 of the 2016 Act, to oversee the whole interception process.

170. Ultimately, sight must also not be lost of the fact that it is open to a person to make a complaint or bring a claim under the HRA to the IPT. The question, therefore, of whether there has been a breach of the HRA on the facts of a particular case is something that can in principle be raised and adjudicated by an independent tribunal which can have access to all relevant material, including secret material. This is another feature of the statutory scheme which persuades us that it is not the 2016 Act itself which can be said in the abstract to be incompatible with the Convention rights.

We also bear in mind in this context that the IPT is itself now subject to the possibility of an appeal to an appropriate appellate court (in England and Wales that would be the Court of Appeal); and that the Supreme Court has recently decided that the IPT is in principle amenable to judicial review: see *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219.

171. The second fundamental complaint which the Claimant makes in the context of bulk interception warrants relates to the definition of "secondary data". The Claimant observes that the concept of secondary data is broader than that of "communications data" under RIPA. The Claimant observes that secondary data can include some data which would have been regarded as "content" under RIPA. This is common ground, although the Defendants do not necessarily accept the full breadth of the examples given in a table produced on behalf of the Claimant.

172. According to that table, examples of secondary data (for the purposes of Part 6, Chapter 1) or non-protected material (for the purposes of Part 6, Chapter 3) which would have constituted content under RIPA include contact "mail to" addresses within a webpage; the location of a meeting in a calendar appointment; information about the photographs such as the time and date and location where they were taken; the full URL of websites visited beyond the "first slash", for example whether someone has been searching on the National Health Service website for such matters as contraception; and what searches they have been conducting on Google or Facebook. Mr Jaffey (who took the lead in making oral submissions on this issue before this Court) also submits that information is regarded as not being "protected material" for the purposes of Part 6, Chapter 3, if it is information that is not private information which may be attached to an email, and that this would exclude (from the definition of "protected material") anything a person has read which is in the public domain, such as a publicly disseminated electronic magazine. Therefore electronic copies of publications such as a newspaper such as the *Socialist Worker* or a magazine such as *Playboy* would not be regarded as protected material for this purpose. This is despite the fact that it may be highly revealing about what a person has been looking at.

173. In our view, this Court must keep firmly in mind that the question which it has to decide in these proceedings is whether the 2016 Act is incompatible with the Convention rights, not (for example) whether it would have been wiser or preferable for Parliament not to include a definition of secondary data which includes some types of what would previously have been regarded as content.

174. In that context, it is particularly important to keep in mind that what this Court has to decide is whether the provisions of the 2016 Act contain sufficient safeguards against the risk of abuse of discretionary power so as to comply with the Convention concept of "law", in particular the requirement of foreseeability. In our view, the fact that bulk interception warrants can include secondary data is compatible with that concept. This is because the Act does contain a set of inter-locking safeguards against the abuse of power. Those safeguards have already been mentioned earlier and, importantly, include the double-lock provisions including the involvement of JCs; and the general oversight regime provided by the IPC.

175. In that context we note that the Defendants have always accepted that the acquisition of secondary data (and previously related communications data under RIPA) is not

"necessarily" less intrusive than the acquisition of content. However, it seems to us that they are entitled to make the point that "as a general rule" the examination of the most sensitive content will raise greater privacy concerns than the examination of secondary data. This has indeed been recognised for many years by the European Court of Human Rights itself: see e.g. *Malone v UK* (1984) 7 EHRR 13, at para. 84.

176. Finally, the point is made on behalf of the Claimant that, where an individual is known to be within the British Islands, but in circumstances where the British Islands safeguard does not apply, it would be possible in principle for the authorities to seek to obtain a bulk interception warrant in circumstances where they ought (according to the Claimant) to seek a targeted warrant.

177. It seems to us that these are the kind of issues which may need to be considered by the Secretary of State and the IPC in considering whether to grant or approve a warrant in the first place. They may also raise issues which may go to the necessity and proportionality and to the auditing of processes by the IPC. Ultimately they may also raise issues which may need to be considered by the IPT on the facts of an individual case.

178. None of that, however, in our view leads to the conclusion that the legislative scheme established by the 2016 Act is itself incompatible with the Convention rights. To the contrary, in our view, it is compatible with the Convention rights, in particular because it creates an important set of inter-locking safeguards which are sufficient to meet the Convention requirement as to the quality of law.

<u>The challenge in respect of bulk and thematic equipment interference warrants</u>

179. On this issue the lead was taken at the hearing before us by Mr Chamberlain on behalf of the Claimant.

180. The statutory provisions governing bulk equipment interference warrants are summarised in the overview in the Annex to our judgment, at paras. 21-24. Further, the general criteria for approval of such warrants (like those relating to bulk intercept and acquisition warrants) are outlined at paras. 25-45 of the overview.

181. In brief, as is apparent from the overview, a bulk equipment interference warrant under section 176(1) of the 2016 Act authorises or requires its addressee to secure any interference with any equipment for the purpose of obtaining "communications", "equipment data" or "any other information"; and has as its main purpose to obtain "overseas-related" communications, information or equipment data. In this context equipment data means either systems data or identifying data (in the case of identifying data subject to the further conditions mentioned at para. 47 above) and is therefore similar to the concept of secondary data in the context of provisions in the Act which relate to bulk interception (see above).

182. Many of the same safeguards apply to such warrants as apply to bulk interception warrants. We would note in particular (para. 44 of the overview) that the Secretary of State must ensure that the selection for examination of "protected material" meets any of the "selection conditions": see section 193(1)(c). This is often known as the

"British Islands safeguard". The selection conditions are as set out in the overview at para. 44(a)-(d).

183. Complaint is made on behalf of the Claimant that this does not include "equipment data", which can in some cases include data which would previously have been regarded as "content".

184. The Claimant makes some fundamental criticisms of the statutory regime for bulk and thematic equipment interference. It submits that the scope and level of discretion conferred by the bulk warrant provisions is the widest of any of the bulk powers in Part 6 of the 2016 Act 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; and a wider range of activities (any "interference" with "equipment"). The Claimant submits that it is also a more serious interference with Article 8 and Article 10 rights because it applies more widely: it enables the retrieval of information which has never been sent via a network and therefore there is an increased expectation of privacy. Further, interference may extend to altering a person's data or their device or the way in which it functions if necessary to retrieve information: see section 176(5). The Claimant submits that the interference may well make the equipment more vulnerable to attack from third parties and relies, in that context, on the evidence of Professor Danezis.

185. In that context Mr Chamberlain makes particular complaint of the fact that such equipment interference may enable the authorities to gain access to stored information which a person has never chosen to transmit (for example photographs, diary entries and notes) and which they may think they have even deleted.

186. On behalf of the Claimant Mr Chamberlain makes two broad submissions:

(1) The 2016 Act contains insufficient safeguards against the risk of abuse of discretionary power and therefore does not comply with the Convention concept of "in accordance with the law".

(2) Further and in any event, the scope of application of the bulk equipment interference power is too wide to be compatible with Articles 8 and 10. It is not necessary in a democratic society because it does not comply with the principle of proportionality.

187. At para. 70 of the Claimant's skeleton argument it appeared to make the submission that the 2016 Act is incompatible with the Convention rights on that second ground irrespective of whether adequate safeguards were attached to it. In that paragraph it was submitted that:

> "the Part 6 Chapter 3 power does not have a sufficiently clear scope of application: it fails sufficiently to limit those who are affected or the basis for the interference. That being so, the power cannot be strictly necessary in a democratic society, even if (contrary to the fact) adequate safeguards were attached to it."

However, at the hearing before this Court, Mr Chamberlain disavowed any such submission. He submitted, as we understood it, that it is because the Act does not contain adequate safeguards that it also fails the test of proportionality.

188. For their part the Defendants submit that the changing nature of electronic communications has made it more important, particularly in a dynamic setting, for the authorities to be able to keep up with the way in which information is stored, for example through encryption and on the so called "dark web".

189. On behalf of the Defendants emphasis is placed on the Bulk Powers Review (August 2016) by Lord Anderson, in particular at paras. 7.1-7.38 on the utility of the power, the reasons why it is needed, and the fact that no alternative may exist to its use. Specifically the Defendants rely on five points:

(1) The fact that the operational case for equipment interference ("EI") lies in the context of diminishing returns from interception owing to developments including end-to-end encryption (100% of emails from major email providers and 50% of internet traffic being encrypted by the time of the Bulk Powers Review) and the increasing anonymisation of network devices, making it harder to distinguish between target and non-target devices with at least some initial analysis of the data held on them.

(2) The fact that bulk EI operations will be designed to bring back the minimum amount of information required to rule out devices not of intelligence interest, which would often imply a "light touch" operation targeted in the first instance on equipment data. It is observed that this is required under section 2 of the 2016 Act, which sets out the general duties in relation to privacy.

(3) The fact that a targeted equipment interference warrant may not be feasible because of the trend towards anonymisation of devices.

(4) The non-viability of covert human intelligence sources ("CHIS") as an alternative in certain scenarios.

(5) Lord Anderson's conclusion, at para. 36, that "an operational case for bulk EI has been made out in principle, and there are likely to be real-world instances in which no effective alternative is available".

190. We should record that the Defendants dispute the evidence of Professor Danezis, which they submit is overstated and in some cases wrong for the reasons given in the second witness statement of Mr Dix, at paras. 10-18. It is unnecessary, in our view, for this Court to resolve such disputes. In the end we have not considered that they have any material bearing on the fundamental issue of compatibility of the 2016 Act with the Convention rights which this Court has to determine.

191. The fundamental argument which is made by Mr Chamberlain is that the mere fact that having a very wide database (sometimes compared at the hearing before us to a "haystack") so that a useful "needle" may be found in it from time to time does not justify the extent of intrusion on privacy which is entailed. He reminds this Court that, in Lord Anderson's Bulk Powers Review (August 2016), at para. 9.9, it was said that:

> "The fact that an intrusive power can be successfully used to avert threats and reduce crime does not of course mean that it should automatically be passed into law: that way lies a police state."

192. In that context, Mr Chamberlain places reliance on the judgment of the Grand Chamber of the European Court of Human Rights in *S and Marper v United Kingdom* (2009) 48 EHRR 50, in which the UK Government argued that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "inestimable value" and produced "enormous" benefits in the fight against crime and terrorism: see para. 92 of the judgment. Indeed this was borne out by specific examples of serious crimes (including murder and rape) which it had been possible to solve because DNA records had been kept of people who had been arrested but never been charged or convicted of a criminal offence. The Court nonetheless held that the retention of such profiles was a disproportionate interference with Article 8 rights: see para. 125.

193. In our view, the decision in *S and Marper* is distinguishable from the present context. First, it concerned the act of actual retention of DNA samples *under* primary legislation, whereas the present case concerns the compatibility of primary legislation with the Convention rights in the abstract. In the present context, it is not possible to say in advance whether or not warrants will be applied for, or granted, under the provisions of the 2016 Act of the breadth which the Claimant asserts could arise in theory. Secondly, the duration of the retention of DNA samples under consideration in *S and Marper* was indefinite whereas in the present context, warrants will usually only last for six months although they can be renewed provided the statutory criteria are met. Further, retention of data will normally only take place for up to two years: see the EI Code, para. 9.31, which is similar in this respect to the Interception Code, para. 9.24. (We note that, under the BPD Code, para. 7.55, there is no specific time limit but copies must be destroyed when the tests of necessity and proportionality are no longer met; and, under the BCD Code, para. 9.13, there is a similar provision to the BPD Code.) Thirdly, what has to be considered in the present context is the entire suite of inter-locking safeguards to which we have made reference earlier. These include the "double lock", including the need for approval by a Judicial Commissioner, and the after the event supervision and potential audit by the office of the IPC.

194. Mr Chamberlain has suggested that the spectre could be raised of a very broadly worded warrant which authorised the security agencies to interfere with the computer software of every person in the whole of a major city like Birmingham so as to download their private diaries. He submits that for the state to require such widespread and indiscriminate collection of private data cannot possibly be consistent with the values underlying the Convention. He submits that this is no different in principle from the state requiring every person in Birmingham under compulsion to provide to the state their paper diaries. If the latter could not properly be done consistent with human rights values, he submits that it cannot be done under the bulk equipment interference regime created by the 2016 Act either.

195. In our view, the answer is provided, as we have already indicated, by the totality of the inter-locking safeguards created by the 2016 Act. The 2016 Act itself is not, in

our view, incompatible with the Convention rights as alleged. Even if the spectre were to arise in practice at some future date, careful consideration would need to be given as to whether there had been a breach of the Convention rights by the *executive* purporting to act *under* the Act.

196. In that context we bear in mind that one of the functions of the IPT (which is an independent judicial tribunal) includes the opportunity to review the acts of the office of the IPC himself. Indeed the Court has before it examples in which the IPT has engaged in precisely such a review in the case of the predecessor commissioners whose functions have now been replaced by the IPC.

197. In support of his submissions Mr Chamberlain relied on the decision of the US Supreme Court in *Riley v California* 573 US _ (2014). That case concerned the issue of whether an exception could be made to the general requirement for a search warrant (pursuant to the Fourth Amendment to the US Constitution) in circumstances where police officers had searched the contents of a cell phone on the arrest of a person. The prohibition of "unreasonable" searches and seizures in the Fourth Amendment generally requires a warrant to be obtained before the police can carry out a search. There are established exceptions to that general rule. One of those exceptions is where a search takes place "incident to an arrest". The question in *Riley* was whether that exception also applied to search of a cell phone of the person who is arrested. The judgment of the Supreme Court was given by Roberts CJ. The Court held that the exception did not apply and therefore a search warrant was required.

198. Mr Chamberlain relied on this decision principally because it illustrates the abhorrence which the American courts have long felt towards "general warrants". As Roberts CJ put it at p.27:

> "Our cases have recognised that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself."

199. The abhorrence for general warrants was of course also clear in the famous cases decided in England in the 18th century, such as *Entick v Carrington* (1765) 19 State Trials 1029. However, in our view, the simple answer to Mr Chamberlain's reliance on cases such as *Riley* is that what the Supreme Court held there was as follows:

> "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant." (p.28).

In other words *Riley* was a case about searches *without* any warrant at all. In the present context Parliament has created a scheme for the grant of warrants in prescribed circumstances which are carefully regulated by the 2016 Act and the codes of practice made under it as well as the supervision of the office of the IPC.

200. That said, before we leave *Riley*, in our view it does provide a helpful reminder of the powerful technology which now exists in (for example) mobile phones and therefore the need for the law to keep up, both in the interests of national security and the protection of the public, and in the interests of the civil liberties of individuals. As Roberts CJ put it, at p.17:

> "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact mini computers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."

He continued, at p.18:

> "The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows just even one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier."

201. Later, at pp.19-20, Roberts CJ also observed that the data stored on a cell phone is distinguishable from physical records by reason of its quality and not only its quantity:

> "An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease … Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."

Non-protected material

202. The second major defect of which Mr Chamberlain complains is the absence of the British Islands safeguard for non-protected material. He submits that the reasoning which prevailed in *Big Brother Watch* in the case of section 8(4) of RIPA can also be read across to the bulk equipment interference regime in the 2016 Act.

203. We do not accept that submission. This is essentially for the reasons we have already set out earlier when rejecting a similar complaint in relation to secondary data in the context of bulk interception warrants.

Thematic equipment interference warrants under Part 5

204. In a separate limb to this challenge Mr Chamberlain also submits that the "thematic" provisions of Part 5 of the 2016 Act are incompatible with the Convention rights. He submits that in some cases thematic equipment interference warrants may be practically indistinguishable from bulk warrants as to their breadth.

205. In that context the Defendants rely upon the decision of the IPT in *Greennet & Ors v Secretary of State for Foreign and Commonwealth Affairs & Ors* [2016] UKIPTrib 14_85_CH, at paras. 54-59. That case concerned what was then called "computer network exploitation". Mr Chamberlain submits that decision is neither binding on this Court nor correct. In any event, he submits that that case concerned section 5 of the Intelligence Services Act 1994 ("ISA"). He submits that the thematic warrant provisions in the 2016 Act can be issued for wider purposes than was possible in the case of section 5 of the ISA. In particular he submits that such warrants may be issued for the purpose of "preventing death or any injury or damage to person's physical or mental health or of mitigating any injury or damage to a person's physical or mental health": see section 106(3).

206. Further, Mr Chamberlain submits that *Greennet* has been overtaken by subsequent developments in Strasbourg, in particular the judgment in *Zakharov*, which was decided in December 2015 but was not taken into account by the IPT, which decided *Greennet* in February 2016.

207. Finally, Mr Chamberlain observes that the High Court (the Administrative Court) has given permission to bring a claim for judicial review of the IPT decision in *Greennet*. The substantive hearing in that case had been stayed pending resolution by the Supreme Court of the question whether the IPT is amenable in principle to judicial review. That issue has now been decided and the substantive claim for judicial review can now proceed in the Administrative Court.

208. Even without regard to the *Greennet* decision, we are not persuaded by these submissions by Mr Chamberlain. We have reached the conclusion that the safeguards in the 2016 Act are sufficient to prevent the risk of abuse of discretionary power and the Act is therefore not incompatible with the Convention rights on the ground that it does not comply with the concept of law. This is essentially for the reasons we have already set out above, as to the totality of the suite of inter-locking safeguards which are contained in the 2016 Act and the codes under it.

209. Further, we accept the submissions made on behalf of the Defendants in this context. They submit that both the 2016 Act and the EI Code of Practice contain provisions as to the need for specificity of warrants. They draw attention to the terms of section 115, in particular subsections (3) and (4). Further they draw attention to para. 5.15 of the Code:

> "The Act requires that certain additional details must be included in the warrant dependent on the subject-matter(s) of the warrant. For example, a thematic warrant that relates to equipment used by a group which shares a common purpose must include a description of that purpose as well as the name or description of as many of the persons who form that group as it is reasonably practicable to name or describe. An equipment interference authority must, when section 115 requires, name or describe as many of the persons, organisations or locations as is reasonably practicable. The description of persons, organisations or locations must be as granular as reasonably practicable in order to sufficiently enable proper assessment of the proportionality and intrusion involved in the interference."

The challenge in respect of bulk personal datasets

210. Bulk personal datasets ("BPD") are governed by Part 7 of the 2016 Act. A detailed summary of the relevant statutory provisions can be found in the overview in the Annex to this judgment, at paras. 79-96.

211. Section 200 generally prohibits an intelligence service from retaining a BPD or examining a BPD it has retained without obtaining a warrant for that purpose, either a "class BPD warrant" or a "specific BPD warrant". Thus, the 2016 Act introduces a new and additional warrant requirement for BPD. Section 201 disapplies that requirement where the intelligence service *obtained* the BPD under a warrant or other authorisation given under the 2016 Act, or the BPD is being retained or examined for the purpose of enabling any information it contains to be destroyed (paras. 80 and 83 of the overview).

212. Under section 199(1) of the 2016 Act, an intelligence service retains a BPD where: (a) it obtains a set of information that includes "personal data" relating to a number of individuals; (b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of intelligence interest; (c) after any "initial examination" of the contents, the intelligence service retains the set of information for the purpose of exercising its functions; and (d) the set is held, or is to be held, electronically for analysis in the exercise of those functions (see para. 79 of the overview).

213. "Personal data" means (a) data within the meaning of section 3(2) of the Data Protection Act 2018 (i.e. relating to an identified or identifiable living individual) which is subject to processing described in section 82(1) of that Act (processing by an intelligence service of personal data wholly or partly by automated means, etc), or (b) data relating to a deceased individual which would fall within (a) if it related to a living individual. Section 220 stipulates time limits for the initial examination of a set of information to determine whether it constitutes a BPD within the meaning of section 199 and, if so, to seek a class or specific BPD warrant. Broadly speaking, the head of an intelligence service has three months to do so where the set of information was created in the UK, and six months where it was created outside the UK.

214. It is common ground that Part 7 does not itself contain any power to *obtain* a BPD. Rather, the requirement for a BPD warrant concerns the retention and any subsequent

examination of a BPD previously obtained under other powers. They may include a warrant issued under section 5 of the Intelligence Services Act 1994 ("ISA"), or exercise of the intelligence services' "information gateway" powers under the ISA and the Security Service Act 1989, and other powers under the 2016 Act (except for Part 6, Chapter 2).

215. The decision to issue either a class BPD warrant or a specific BPD warrant must be taken by the Secretary of State personally (section 211) and is subject to prior approval by a JC, except where the Secretary of State considers there is an "urgent need" for a specific BPD warrant to be issued (sections 204(3)(e), 205(b)(e) and 208). Where a specific BPD warrant is issued without prior JC approval because of urgent need, the Secretary of State must inform a JC that the warrant has been issued and, within three working days, the JC must decide whether or not to approve that decision. In the event of a refusal to approve the warrant, it ceases to have effect (section 209). The JC may direct the destruction of data retained under the warrant or impose conditions as to the use or retention of such data (section 210).

216. A class BPD warrant authorises the retention or examination of any BPD falling within a class described in the warrant; whereas a specific BPD warrant authorises the retention or examination of any BPD described in that document. Neither type of BPD warrant may be issued (or approved) unless both the Secretary of State and the JC consider that it is necessary on the grounds of national security, for the prevention or detection of serious crime, or in the interests of the economic well-being of the UK in so far as those interests are also relevant to national security. They must also be satisfied that the operational purposes specified in the application for the warrant are purposes for which examination of the BPD described is or may be necessary, and that such examination is necessary on any of the grounds upon which the warrant is considered necessary. In addition, both the Secretary of State and the JC must be satisfied that the conduct authorised by a warrant would be proportionate to what is sought to be achieved (see sections 204(3), 205(6) and 208(1) and (2)).

217. Furthermore, the general duties in relation to privacy in section 2 are engaged. Thus, the Secretary of State and the JC must consider whether what is sought to be achieved by the warrant could be achieved by other less intrusive means. They must also consider any aspect of the public interest in the protection of privacy (section 2(2)) and any consideration relevant to proportionality (section 2(3) and (4)). The JC must consider these matters with a sufficient degree of care as to ensure that he or she complies with the duties under section 2 (section 208(2)(b)).

218. Thus, the issuing of BPD warrants under Part 7 is subject to many of the fundamental safeguards in Part 6 to which we have already referred, including, in particular, the "double-lock" provisions.

219. Furthermore, a BPD may not be retained, or retained and examined, pursuant to a class BPD warrant if the head of the intelligence service considers that the BPD consists of or includes, "protected data" or "health records" (section 206) or that a substantial proportion of the BPD consists of "sensitive personal data". Essentially, "protected data" means (section 203) "private information" (which "includes information relating to a person's private or family life" and all other data in a BPD other than "systems data" or "identifying data" which is capable of being separated logically from that BPD without revealing the meaning of any of the data). An application to retain, or to

retain and examine, data within these categories would have to be made as an application for a specific BPD warrant. Additional safeguards in relation to specific warrants covering "health records" and "protected data" are provided by sections 206 and 207 (see the overview at para. 90).

220. In relation to bulk warrants issued under Chapters 1, 2 or 3 of Part 6, the Secretary of State must consider that satisfactory arrangements are in force for securing safeguards relating to access to, copying, examination and destruction of material (sections 138(1)(e), 158(1)(d) and 178(1)(e); and see the overview, at paras. 37-38). These safeguards are more specifically defined in sections 150-1, 171 and 191-2. By contrast, for BPD warrants issued under Part 7, the Secretary of State need only consider that the arrangements made by the intelligence service for storing the BPD or BPDs to which the application relates and for protecting them from unauthorised disclosure are satisfactory (sections 204(3)(d) and 205(6)) and the statute does not go on to lay down any more specific requirements. Nevertheless, there are specific additional safeguards for the examination of BPD or data subject to legal privilege (sections 221-223; and see also paras. 92-95 of the overview).

221. Sections 213-219 deal with the duration, renewal, modification and cancellation of BPD warrants (paras. 90-91 of the overview). Save for section 219, which we consider below, these provisions largely mirror those applicable to bulk warrants under Part 6.

222. In his Bulk Powers Review (August 2016) Lord Anderson said that he had no hesitation in accepting that BPDs are of great utility to the intelligence services. The case studies which he examined, and which we were shown in Appendix 11, provided unequivocal evidence of this. BPDs enable targets to be identified and swift action to be taken to counter a threat. The obtaining of accurate information at great speed has a considerable value. Many alternatives would be slower, less comprehensive or more intrusive. In some areas, particularly pattern analysis and anomaly detection, no practicable alternative to the use of BPDs exists. Where an agency does not have the "seed" of intelligence usually needed to begin an investigation, these techniques enable it to spot hostile activity or actors. The case studies provided examples of the identification of serious threats which would not have been possible without the use of BPD. In other cases, an agency was able to identify a hostile person from a "partial identifier" using BPD.

223. At the outset of the hearing before us Mr Chamberlain submitted that the BPD powers conferred by Part 7 are too wide to be compatible with Articles 8 and 10 because virtually any data could be retained and examined under a BPD warrant so long as it comprises personal data held electronically (paras. 106-9 of the Claimant's skeleton). By way of example, he said that the language of the legislation is so broad to allow the authorisation of the kind of national DNA or fingerprint data base which was held to be unlawful in *S and Marper* and *MK v France* (Application No 19522/09, judgment of Fifth Section, 18 April 2013). He submitted that the safeguards relate solely to examination and not to the authorisation of retention.

224. We do not accept these submissions. As we have already indicated, the question for this Court is whether the *legislation* as enacted, and not actual practices or activity, is incompatible with Articles 8 or 10. Here the key issue for us is whether the legislation indicates the scope of the powers conferred and the manner in which they may be

exercised with sufficient clarity to give adequate protection against "arbitrary interference" (*Zakahrov*, at para. 230). The statutory requirement that both the Secretary of State and the independent JC have to apply necessity and proportionality tests to a properly formulated application is designed to ensure that retention of the kind which was found to be in breach of the ECHR in *S and Marper* or in *MK* would not be authorised and would therefore be prohibited by section 200. Our conclusion is similar to that which we reached on the challenge regarding the general and indiscriminate retention of data under Part 4 of the 2016 Act (see [2019] QB 481, at para. 135). It is wrong as a matter of principle to argue that Part 7 is incompatible with Articles 8 and 10 by advancing factual scenarios which would be incompatible with legal principles (and independent mechanisms to give effect to those principles) enshrined in the Act itself.

225. We have reached a similar conclusion on the Claimant's related argument that the legislation gives the Secretary of State a choice as to whether to issue a warrant for the retention of a BPD either in the form of a class BPD warrant or a specific BPD warrant. A class warrant is simply required to describe the class of BPD to which it relates without saying how a "class" is to be defined (para. 115 of the Claimant's skeleton). We agree with the Defendants that if on a given set of facts it is not necessary or proportionate to issue a class BPD warrant because a less intrusive specific BPD warrant could be issued to address the purpose of the application, then neither the Secretary of State will be able to issue, nor a JC to approve, the issuing of a class BPD warrant (see para. 91(3) of the Defendants' skeleton).

226. This conclusion is reinforced by paras. 5.3-5.5 of the Code of Practice on retention and use of BPD's. If the JC or the Secretary are not satisfied as to the nature and scope of a class, or the number of BPDs which may fall within the class, the application for a class warrant may be refused or it may be granted subject to conditions which reduce the ambit of the class. Alternatively, the intelligence service may be required to split the class for which a warrant is sought and to submit revised applications for smaller class BPD warrants so as to ensure effective oversight. Such outcomes are the direct result of applying the necessity and proportionality tests embedded in the statutory framework and machinery for the authorisation of warrants.

227. As we have previously explained, Part 7 neither authorises an agency to *obtain* data, nor to *retain* data which could not otherwise be retained under other legislation. Instead, it requires the retention of BPD previously obtained under other regimes to be subjected to the safeguards introduced by Part 7, not least the "double lock provision", requiring independent scrutiny and approval through the warrantry procedure, and the subsequent monitoring of the audit process of the powers used. As the Defendants point out, there is no challenge before the court to the regime in the ISA or the Security Service Act 1989.

228. Next the Claimant criticises Part 7 for failing to include the British Islands safeguard for the examination of BPDs, especially in view of the fact that this power does not have to be exercised mainly in relation to "overseas-related communications" (as, for example, in the case of bulk interception warrants). Instead, section 207 merely gives the Secretary of State a power to impose conditions when issuing a "specific" BPD warrant which must be satisfied before "protected data" may be selected for examination by criteria referable to an individual known to be in the British Islands. We note that where that power is exercised, section 221(3) then requires the Secretary

of State to ensure that arrangements are in force for seeing that any selection of protected data by reference to such criteria accords with the conditions specified under section 207.

229. To put this point into context, we recall that under the 2016 Act the British Islands safeguard applies to the selection for examination of "intercepted content" (section 152(1)(c) and (3)) or "protected material" (section 193(1)(c) and (3)) obtained from a bulk interception warrant or a bulk equipment interference warrant. It does not apply to the examination of "secondary data" or "non-protected material". We have previously explained why we reject the Claimant's criticism of these provisions, that the safeguard no longer applies to material previously treated as "content" for the purposes of section 8(4) of RIPA and why we reject the Claimant's attempt to read across conclusions on RIPA reached by the First Section in the *BBW* case to the 2016 Act.

230. The Defendants respond that in general BPDs do not contain material defined as "content". Nevertheless, the Bulk Powers Review (August 2016) acknowledged that a "small proportion" of BPD does contain "content" (para. 2.71) and it is common ground that the examination of metadata may sometimes be as intrusive as "content".

231. We see no force in the criticisms which the Claimant makes and certainly nothing which could justify a finding of incompatibility of the 2016 Act with Articles 8 and 10. The concept of "protected data" for the purposes of BPD warrants is similar to "protected material" (section 193(9)) for the purposes of bulk equipment interference warrants. These concepts are similar to "intercepted content" (section 157(1)) for the purposes of bulk interception warrants, save that they also expressly include "private information" even if that material would otherwise be excluded from the British Islands safeguard as "systems data" or "identifying data".

232. As we have pointed out, an intelligence service may not rely upon a class BPD warrant to authorise the retention, or the retention and examination, of a BPD if that dataset consists of, or *includes*, "protected data". Accordingly, we do not need to consider the British Islands safeguard further in relation to class BPD warrants.

233. Where a BPD includes "protected data", and therefore could include "content", the intelligence service will need to apply for, and obtain, a specific BPD warrant to authorise the continued retention of that material, or any examination thereof. It is because of this distinction between "class" and "specific" BPD warrants that the power in section 207 to impose conditions controlling selection for examinations by criteria referable to an individual known to be in the British Islands applies solely to applications for specific BPD warrants.

234. We agree with the Defendants' submission that the issue of whether a British Islands safeguard should be included in a specific BPD warrant by imposing conditions on the warrant is a matter that falls to be considered not only by the Secretary of State but also by the JC applying the tests of necessity and proportionality under section 208. That "double lock" and the set of inter-locking safeguards generally to be found in the 2016 Act provide sufficient protection under the Act to avoid arbitrary interference with rights under Articles 8 or 10.

235. Furthermore, an intelligence service may not rely upon a class BPD warrant for the retention of a BPD where the head of that service considers that the BPD consists of, or includes, health records (as defined in section 206) or that a substantial proportion of the BPD consists of "sensitive personal data", that is personal data comprising information about an individual (whether living or deceased) of a kind mentioned in section 86(7)(a)-(e) of the Data Protection Act 2018 which identifies an individual through genetic or biometric material, or concerns an individual's health, sex life or sexual orientation, or reveals their political opinions, religious or philosophical beliefs, racial or ethnic origin, or trade union membership (section 202(4)).

236. The Claimant criticises section 219 of the 2016 Act, which deals with the situation where a BPD warrant ceases to have effect because it expires without having been renewed or because it is cancelled. The legislation allows for retention of BPD for limited periods of time, for example until the determination of an application for a new BPD warrant. It is said that the legislation does not restrict the examination of any material so retained during such periods to the operational purposes specified in the warrant which has ceased to have an effect.

237. In our judgement it is necessarily implicit in the statutory scheme that section 219, which is only a temporary "bridging" provision during the period when a decision is being taken whether to apply for a fresh warrant and any such application is being considered, could not be used to circumvent the safeguards in the 2016 Act, including the "operational purposes" restriction. Accordingly, it is necessarily implicit that any examination of BPD material whilst section 219 applies would have to be necessary for one or more of the operational purposes and the grounds in relation to which the warrant was granted. Section 219 could not be relied upon so as to circumvent that requirement. As the Defendants rightly point out (para. 92 of their skeleton), examination of material retained in reliance upon section 219 would in any event be constrained by the principles of necessity and proportionality through the obligation in section 6 of the HRA, as confirmed by section 2 of the 2016 Act, including its explicit reference to section 219(3).

238. A BPD warrant may last for six months (section 213). Section 214 of the 2016 Act allows for the renewal of a BPD warrant subject to meeting (among other things) the tests of necessity and proportionality and, in relation to examination of BPD, the same purpose tests as were applied when the warrant was granted. There is an overall safeguard that any renewal requires the approval of a JC. A warrant may be renewed for six months. Para. 7.55 of the relevant Code of Practice provides that, where the continued retention of BPD no longer meets the tests of necessity and proportionality, all copies, extracts and summaries of it, must be scheduled for destruction as soon as possible, for example, once it is no longer needed for any authorised purpose. These safeguards are sufficient for compatibility with Articles 8 and 10.

239. Lastly in relation to the BPD regime, the Claimant criticises section 225. This empowers the Secretary of State to give a direction in effect applying Part 7 to BPD obtained by an intelligence service under another Part of the 2016 Act (except Chapter 2 of Part 6) in place of the powers and regulatory provisions of that Part. The Secretary may include a provision in such a direction that any of the regulatory provisions in another Part of the 2016 Act that previously applied to the retention, examination, disclosure or other use of BPD shall continue to apply, with or without modification (section 225(5) and (14)). Any direction under section 225 can only be

made with the approval of a JC (section 225(7)). Furthermore, the intelligence service may only retain, or retain and examine, the BPD if so authorised by a class BPD warrant or a specific BPD warrant (section 225(4)), which would also require approval by a JC. Any direction under section 225 cannot interfere with the continued application of the safeguards in sections 56-59 of the 2016 Act.

240. In our judgement the "double lock" provisions and other safeguards contained in Part 7 of the 2016 Act are sufficient to prevent arbitrary interference with rights under Articles 8 and 10. We have concluded that those safeguards are adequate where BPD has been obtained under provisions not contained in the 2016 Act. We are also satisfied that the regime established by that Act is adequate to ensure that BPD is not brought within the scope of Part 7 from other parts of the 2016 Act without ensuring that sufficient safeguards continue to apply to the retention and use of that data.

The challenge in respect of bulk acquisition warrants

241. Chapter 2 of Part 6 provides for the issuing of bulk acquisition warrants which authorise the obtaining, imposition of a requirement to obtain, and selection for examination and disclosure of "communications data" ("CD"). A detailed summary of the relevant statutory provisions may be found in paras. 17-20, 25-43 and 45 of the overview in the Annex to this judgment.

242. Specifically, a bulk acquisition warrant authorises or requires its addressee to secure, by any conduct described in the warrant, any one or more of the following (see section 158(5) and (6)):

a) requiring a telecommunications operator specified in the warrant (i) to disclose to a person specified in the warrant any CD which is specified in the warrant and is in the possession of the operator, (ii) to obtain any CD specified in the warrant which is not in the operator's possession but which the operator is capable of obtaining, or (iii) to disclose to a person specified in the warrant any data so obtained;

b) the selection for examination, in any manner described in the warrant, of CD obtained under the warrant;

c) the disclosure, in any manner described in the warrant, of CD obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

243. CD essentially constitutes data that enables the intelligence services to understand matters such as "who has been communicating with whom, and where from, as [opposed to] what the parties actually said to one another" (Lord Anderson's report, "A Question of Trust" (June 2015), para. 5.26).

244. Lord Anderson concluded in para. 6.47 of his Bulk Powers Review (August 2016) that it had been demonstrated that powers for the bulk acquisition of CD are crucial in a variety of fields, including counter-terrorism and counter-espionage. The case studies he cited gave examples in which bulk acquisition had contributed significantly to the

disruption of terrorist operations and the saving of lives. By providing swift target identification, bulk acquisition is valuable for dealing with imminent threats. Even where alternative methods may be available, they are often more intrusive. Many of the alternatives which had been suggested would be far slower and less efficient than bulk acquisition (para. 6.35), which also may provide more accurate results than targeted techniques (para 6.30).

245. Mr Dix also explains the importance of bulk acquisition of CD at paras. 210 to 220 of his first witness statement. He states that these techniques are used to identify subjects of interest within the UK and overseas, so as to understand relationships between suspects in a way that would not be possible using only targeted CD. For example, bulk CD enables the intelligence agencies to search for traces of activity by suspects who were previously unknown but who surface during the course of an investigation. Identifying links and methods in this way can help to indicate whether other investigatory powers, such as interception, need to be used.

246. The safeguards applicable to the issuing of bulk acquisition warrants are generally similar to those relating to bulk interception and bulk equipment interference warrants. The Secretary of State must be satisfied that the warrant is necessary in the interests of national security, or on that ground together with the prevention or detection of serious crime, or the interests of the economic well-being of the UK in so far as those interests are also relevant to national security. He must also be satisfied that the conduct authorised by the warrant is proportionate to what is sought to be achieved, that each of the specified "operational purposes" is a purpose for which the examination of material obtained under the warrant is or may be necessary and that the examination of material for such a purpose is necessary for any of the grounds on which the warrant is considered to be necessary. Operational purposes may only be drawn from the list of purposes approved by the Secretary of State and maintained by the heads of the intelligence services, supplied to the ISC every three months and reviewed by the Prime Minister annually. Para. 4.5 of the relevant Code of Practice sets out the matters which must be addressed in an application to the Secretary of State for a warrant under Chapter 2 of Part 6. The same information must also be placed before the JC who considers the application (para. 4.13).

247. The Secretary of State must also be satisfied that arrangements are in force for the purposes of the safeguards under sections 171 and 172 relating to the manner in which data is retained or selected for examination and its disclosure. In particular, by section 172, those safeguards must secure that any selection of CD for examination is necessary and proportionate and is carried out solely for the operational purposes specified in the warrant as originally approved by the Secretary of State and the JC (or as subsequently modified under the approval procedures laid down by sections 164-6).

248. The warrant cannot be issued without the approval of a JC (sections 158 and 159). The decision to issue the warrant must be taken by the Secretary of State personally (section 160).

249. "Communications data" is defined by section 261(5) in relation to a telecommunications operator, system or service as meaning either "entity data" or "events data" but it does not include any "content" of a communication (or anything which would be treated as "content" if it were not otherwise treated by the legislation as "systems data": see section 261(5)(c) and (6)(b)). "Entity data" and "events data"

are defined in section 261(3) and (4) so as to be mutually exclusive. These concepts have previously been considered by this Court in its judgment at [2019] QB 481, paras.140ff.

250. An "entity" means a person or thing (section 261(7)). In summary, "entity data" means any data which is about an entity or a link between an entity and a telecommunications service or part of a telecommunications system, or which comprises data identifying or dealing with that entity (section 261(3)). "Events data" means (in summary) any data identifying or describing an activity carried on by one or more entity on, in, or by means of a telecommunications system (section 261(4)). These two definitions have to be read together with the definition of CD in section 261(5), which further delimits the ambit of the regime under Chapter 2 of Part 6. Thus, in essence, CD refers to entity or events data which is:

a) held, or capable of being held or obtained by, a telecommunications operator and relates to the provision of a telecommunications service to an entity, or is comprised in or associated with a communication for the purposes of the system by which that communication is sent, or otherwise relates to the use of a telecommunications service or system; or

b) comprised in or associated with a communication for the purposes of the telecommunications system by which it is sent and is available directly from that system; or

c) is about the architecture of the telecommunication system, but is not about a specific person.

251. As Sir James Eadie explained, in the 2016 Act Parliament has consciously moved away from the approach taken in earlier legislation. More safeguards have been introduced and a tiered approach has been taken to the application of those safeguards. First, there is "content", the data which generally (not, it is common ground, always) has the greatest potential overall for intrusion into privacy or interference with Convention rights and therefore is in the highest tier. Secondly, there is the combination of "systems data" and certain "identifying data" which together make up "secondary data" in the case of bulk interception and "protected material" in the case of bulk equipment interference. Thirdly, and in the lowest tier, there is the category "communications data" (as defined in section 261(5)) in the narrower field of telecommunications, a source which for many years has been relied upon in criminal investigations. GCHQ's 'Compliance Guide (2018)' describes CD as a "subset of systems data" (p.244).

252. This categorisation was helpfully elaborated in a Note on behalf of the Defendants produced on the fifth day of the hearing. The British Islands safeguard only applies to "intercepted content" (section 152(1)(c) and (3)-(5)) and "protected material" (section 193(1)(c) and (3)-(5)). Both of these definitions are focussed on "content". The British Islands safeguard does not apply to "secondary data" (bulk interception warrants) or to non-protected material (bulk equipment interference warrants).

253. Content is defined in section 261(6) as meaning "any element of the communication, or any data attached to or logically associated with the communication, which reveals

anything of what might reasonably be considered to be the meaning … of any communication….".

254. Then taking "secondary data" by way of example, the first component, "systems data", is data which broadly speaking enables or facilitates the functioning of a system. In some instances (said by the Defendants to be "limited"), "systems data" may also reveal something of the meaning of a communication, but such data is treated as "systems data" and excluded from "content" (see section 261(6)(b)).

255. Turning to the second component of "secondary data", the Defendants' Note states that "identifying data" will often amount to "content" because it will reveal aspects of the meaning of a communication. Because of the extent of this overlap with "content", "secondary data" only includes "identifying data" which is "logically separable" from the communication and, if so separated, would not reveal anything of what might reasonably be considered to be its meaning, or "content". "Identifying data" which is not so separable from a communication or, if separable, would reveal the meaning of that communication falls outside the definition of "secondary data" and so may qualify as "intercepted content" (or as "protected material" under Chapter 3 of Part 6), thereby attracting the British Islands safeguard in the 2016 Act (as well as the other safeguards in the 2016 Act).

256. Under the tiered approach to data, "secondary data" and non-protected material do not attract the British Islands safeguard, but they are protected by the other key safeguards, including the safeguards relating to the issuing of a warrant, JC approval, the operational purposes test, the necessity and proportionality tests, the arrangements for securing safeguards on the retention and examination of material, and IPC oversight.

257. The third category of data to which the bulk powers under Part 6 of the 2016 Act apply is CD. We have already summarised the detailed set of definitions which circumscribe the ambit of this category. It is important to emphasise that data falling within the definition of "content" (section 261(6)) is excluded from the ambit of CD. Thus, the bulk powers under Chapter 2 of Part 6 cannot be relied upon to authorise the acquisition, selection for examination, or disclosure of "content". We accept the Defendants' submission that, viewed overall, this third category is less sensitive in nature than either the first category (intercepted content or protected material) or the second category (secondary data or non-protected material).

258. Because the bulk acquisition of CD regime cannot apply to "content", Chapter 2 of Part 6 does not employ the British Islands safeguard. That safeguard applies in the bulk interception and bulk equipment interference provisions but only in relation to the selection for examination of intercepted content or protected material. Thus, the non-availability of the British Islands safeguard in Chapter 2 is consistent with the legal basis upon which it is made available in Chapters 1 and 3.

259. In contrast to Chapters 1 and 3 of Part 6, a warrant for bulk acquisition of CD need not have as its main purpose the interception of overseas-related communications or information or related secondary material. The main criticism made by the Claimant of the powers in Chapter 2 is that they do not contain a British Islands safeguard, so that they may be used to target and examine data relating to a person present in the British Islands, rather than using dedicated powers elsewhere in the Act. The

Claimant also relies upon the decision of the First Section in *Big Brother Watch*, at para. 357, in relation to RIPA sections 8(4) and 16.

260. For reasons which we have already given, we do not accept that the Court's conclusions in *Big Brother Watch* can be read across to the 2016 Act. Chapter 2 of Part 6 replaces the loosely structured regime in section 94 of the Telecommunications Act 1984. The current legislation imposes a set of detailed, inter-locking safeguards as summarised above which did not previously apply, either under the 1984 Act or indeed under RIPA.

261. The Claimant's argument focuses on the examination of CD. We do not accept that the safeguards applicable to such an examination, absent a British Islands safeguard, fail to provide adequate protection against arbitrary interference with rights under Articles 8 or 10 of the ECHR.

262. A bulk acquisition warrant must specify not only the statutory grounds for which the warrant is necessary, but also the operational purposes for which any CD acquired under the warrant may be selected for examination. The warrant must be approved by the Secretary of State and a JC applying the necessity and proportionality tests. Sections 171 and 172 require that arrangements are in force for securing that data is selected for examination solely for operational purposes specified in the warrant and where examination is necessary and proportionate. The Code of Practice for Bulk Acquisition of CD (para 6.15) requires records to be kept which enable compliance with section 172 to be audited by the IPC acting under section 229. In our judgement the legal framework applicable to bulk acquisition of CD provides sufficient independent oversight of selectors and search criteria, so as to overcome the criticism made of the regime governing section 8(4) of RIPA in *Big Brother Watch*, at para. 340.

263. The Claimant criticises section 171(7)-(10) of the 2016 Act which, in effect, enables the Secretary of State to disapply the safeguards in section 171(2) and (5) and section 172 in relation to data disclosed or copied to overseas authorities. These safeguards are concerned with limiting the copying of and access to data, selection for examination of data, and the destruction of data when no longer required.

264. In the light of the reasoning of the majority of the IPT in the *Privacy International* case [2018] UKIPTrib 15_110-CH (paras. 61ff) in relation to the regime under section 94 of the Telecommunications Act 1984, and having regard also to paras. 9.10-9.12 of the Code of Practice for Bulk Acquisition of CD, we see no basis for this Court to conclude that Chapter 2 of Part 6 is not in accordance with the law and therefore incompatible with Articles 8 or 10 of the ECHR.

<u>The challenge to Parts 3 and 4 of the 2016 Act</u>

265. Part 3 of the 2016 Act sets out the procedures and circumstances in which certain specified public authorities may obtain "communications data". Section 60A empowers the IPC to grant applications for authorisation made by certain public bodies on designated grounds, which include national security and the prevention or detection of serious crime. Section 61 empowers designated senior officers within

certain public bodies to authorise the obtaining of CD. Section 61A deals with authorisation in urgent cases. These provisions are summarised in paras. 103-106 of the overview in the Annex to this judgment.

266. Part 4 of the 2016 Act empowers the Secretary of State to serve a retention notice requiring a telecommunications operator to retain certain CD for periods of up to 12 months. The relevant provisions are summarised in paras 99-101 of the overview. The issue of whether Part 4 complies with EU law was dealt with in the judgment of this Court at [2019] QB 481. The amendments which have been made to Part 4 in response to that judgment are summarised in paragraph 100 of the overview.

267. The Claimant made a number of submissions in its pleadings and skeleton. In their corresponding documents the Defendants replied to the points made. The Claimant did not develop any of its contentions at the hearing and so we did not hear oral arguments on these matters. In these circumstances, it would be inappropriate for the Court to address each of the points raised or to deal with this part of the challenge in any detail. Once again, it has to be borne in mind that the issue for the Court is whether the Claimant can demonstrate that these provisions are not in accordance with law or are intrinsically disproportionate so as to justify a declaration of incompatibility.

268. In summary, the Claimant contends that the purposes for which the powers in Parts 3 and 4 may be exercised are too wide, the range of authorities that may obtain CD under Part 3 is too wide, and certain procedures under Part 4 are insufficiently clear and detailed. We do not accept any of the points raised.

269. We have regard to the safeguards in both Parts 3 and 4 summarised in the overview and to the analysis of Part 4 at 2019 QB 481, at paras. 127-135. That analysis is also relevant to the issue of compatibility with the ECHR.

270. We do not accept the suggestion that the purposes for which Parts 3 and 4 may be exercised are too wide or arbitrary. First, those purposes were reduced in scope by the Data Retention and Acquisition Regulations 2018. Secondly, the powers are concerned with "communications data". Thirdly, the powers in Parts 3 and 4 are subject to the necessity and proportionality tests. Fourthly, the powers are subject to JC or OCDA approval where necessary. Fifthly, certain of the powers are limited to specific operations or investigations (see s.61(1)(b)). Sixthly, the mere fact that under Part 3, powers may be obtained by a range of public authorities does not support an argument of incompatibility. The key consideration is what are the relevant powers, procedures and safeguards, and how are they defined. We have not seen anything in the material put before us to indicate that Parliament has enacted legislation giving rise to the risk of arbitrary interference or any other incompatibility with the Convention rights.

Lawyer-client communications

271. Decisions on warrantry and authorisations under Parts 2, 3, 4, 5, 6 and 7 of the 2016 Act are subject to the general duties in section 2 in relation to privacy. A "public authority" (as defined in section 6 of the HRA: see section 263(1)), which includes the

Secretary of State, the IPC and a JC, must have regard, amongst other things, to "whether the level of protection to be applied in relation to the obtaining of any information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of the notice" and "any other aspects of the public interest in the protection of privacy" (section 2(2)(b) and (d)). The duties under section 2(2) are subject to the need to have regard to other relevant considerations (section 2(3)), which include the necessity and proportionality tests, and the requirements of the HRA (section 2(4)). For the purposes of section 2(2)(b), "sensitive information" includes "items subject to legal privilege" (section 2(5)). Thus, the need to treat such items as sensitive is a principle which suffuses the entire regime in the 2016 Act.

272. Section 263(1) defines "items subject to legal privilege". No issue has been taken over the ambit of that definition.

273. The Act also contains specific safeguards in relation to items subject to legal privilege. These are summarised in the overview in the Annex to this judgment, at paras. 46-51 (as regards Chapters 1 and 3 of Part 6 of the 2016 Act), para. 57 (as regards Chapter 2 of Part 6), paras. 48 and 74 (as regards Part 5), and para. 94 (as regards Part 7).

274. In broad terms the additional safeguards under Chapters 1 and 3 of Part 6 apply where it has not been necessary to obtain a targeted examination or interception warrant in order to address the British Islands safeguard (sections 152(1) and (6), 194 (1) and (6)). Where such a warrant is needed, parallel safeguards are contained in Part 5.

275. Two of the safeguards for bulk interception and equipment interference powers apply to selection for examination of "intercepted content" and "protected material".

276. Under the first safeguard, where a purpose of the criteria to be used for selecting such material for examination is to identify items subject to legal privilege, or the use of those criteria is likely to reveal such items, a "senior official" acting on behalf of the Secretary of State must approve the use of those criteria (sections 153(2) and 194(2)). That official must have regard to the public interest in the confidentiality of such items (section 153(3) and section 194(3)). No such approval may be given unless the official considers that the arrangements under section 150 or section 191 include safeguards for the handling, retention, use and destruction of such items. Additionally, where the purpose is to identify items subject to legal privilege, the official must be satisfied that there are "exceptional and compelling circumstances" making it necessary to authorise the use of those selection criteria (section 153(4) and section 194(4)). That test is not satisfied unless the official is satisfied that the public interest in the selection for examination outweighs the public interest in the confidentiality of "items" subject to legal privilege, there are no other means by which the information may reasonably be obtained, and the information is necessary for national security or to prevent death or significant injury (section 153(5) and section 194(3)).

277. Under the second safeguard, where a purpose of the criteria to be used for selecting "intercepted content" or "protected material" for examination is to identify communications that would be subject to legal privilege if they were not made in order to further a criminal purpose, those criteria may not be used unless approved by a senior official acting on behalf of the Secretary of State and that person considers that the targeted communications are likely to have been made with the intention of furthering a criminal purpose (section 153(6)-(8), section 194(6)-(8)).

278. Under the third safeguard, where an item subject to legal privilege has been intercepted under Chapter 1 or obtained under Chapter 3 and is retained following its examination, other than to be destroyed, the IPC must be informed as soon as reasonably practicable (section 153(9) and section 194(9)). The IPC must either direct the destruction of the item or impose conditions on its use or retention (section 153(10) and section 194(10)), unless he considers that the public interest in retaining the items outweighs the public interest in the confidentiality of "items" subject to legal privilege and that retention is necessary for national security or for preventing death or significant injury (section 153(12) and section 194(12)). Even where he does so consider, the IPC may still impose conditions on the use or retention of the items in order to protect the public interest in the confidentiality of legal privilege (section 153(11) and section 194(11)). It is to be noted that the application of the third safeguard is not limited to "intercepted content" or "protected material"; it applies generally to any item subject to legal privilege which has been intercepted or obtained under Chapters 1 or 3 of Part 6.

279. Similar provisions to the first two safeguards described above have been enacted in sections 27 and 112 for targeted interception or examination or mutual assistance warrants and targeted equipment or examination warrants under Parts 2 and 5 respectively. Save in urgent cases, such warrants are subject to the "double lock" and so require prior approval by a JC (sections 19, 23, 102 and 108). In urgent cases, subsequent JC approval must be sought in any event. A JC has independent powers to order destruction of legally privileged material or to impose conditions on its use or retention (sections 24-25 and 109-110). Furthermore, similar provisions to the third safeguard described above have been enacted in sections 55 and 131 in relation to targeted (and mutual assistance) warrants under Parts 2 and 5 respectively. The provisions mentioned in this paragraph are not directed specifically to privileged items and apply to all material obtained under an urgently issued warrant.

280. In the case of a "specific" BPD warrant, similar provisions to the three safeguards we have described for Chapters 1 and 3 of Part 6 have been enacted for Part 7 (sections 222-223). In addition, section 222(2) and (10) allow the use of selection criteria referable to a person known to be in the British Islands at the time of selection, subject to the approval of a JC (as well as the Secretary of State). However, JC approval is not required where material is being selected for examination which is likely to have been created or held with the intention of furthering a criminal purpose (section 222(4), (8) and (12)).

281. It can therefore be seen that a wide range of dedicated and detailed safeguards for legally privileged items have been enacted under Parts 2, 5 and 6 (Chapters 1 and 3). But we note that Parliament has decided not to provide the first or second safeguards in relation to the *bulk* acquisition of secondary data or non-protected material (Chapters 1 and 3 of Part 6) or a "class" BPD warrant (under Part 7).

282. Furthermore, Parliament has decided not to provide any of the three safeguards for the bulk acquisition of CD (Chapter 2 of Part 6). However, for that type of bulk acquisition the relevant Code of Practice states that the general privacy duties in section 2 are engaged. The Code makes plain the sensitivity of legally privileged items, the need for "special consideration" in the application of the necessity and proportionality tests and for particular care in the treatment of such items (paras 6.19-6.23).

283. We will focus on the submissions made by Mr Jaffey during the hearing. He described the third safeguard for legally privileged items (see e.g. section 153(9) to (12)) as "strong". We agree. However, he criticised the legislation, first, for failing to provide safeguards in relation to the bulk acquisition of "secondary data" and "non-protected" material and data (Chapters 1 and 3 of Part 6 and Part 7); and, secondly, for the bulk acquisition of CD (Chapter 2 of Part 6).

284. We put to one side for the moment CD. We proceed on the basis that it may be possible to identify from secondary data and non-protected material or data who has been communicating with whom and when. So, Mr Colin Passmore, a partner in Simmons & Simmons, explained in his witness statement that it would be possible to identify the fact that a client has consulted a lawyer, or the fact that advice has been taken, or the fact that a solicitor has contacted a potential witness in litigation.

285. There was a dispute as to how exceptional or otherwise such examples of legal privilege may be. We do not need to resolve this. Even if legally privileged items falling outside the scope of "content" are intercepted or obtained under a warrant, they are subject to the "third safeguard" in section 153(9)-(14) and also sections 55, 131, 194(9)-(14) and 223. The IPC must apply the dual tests of whether (a) the public interest in retention outweighs the public interest in the confidentiality of legally privileged items and (b) retention is necessary for national security or for preventing death or significant injury. Subject to the outcome of the IPC's assessment applying those tests, the Commissioner may direct destruction of the items in question or the imposition of conditions on their retention or use.

286. The requirement under that third safeguard for both tests to be applied, if a legally privileged item is intercepted or obtained, also meets in substance the Claimant's criticism that the first safeguard does not require those tests to be applied where the use of selection criteria for examination is only "likely to identify" legally privileged items, as opposed to its being a purpose of using those criteria to identify such items. In this context, we also bear in mind the overarching requirements of the general duties in relation to privacy, notably section 2(2)(a)(b) and (d), (4)(c) and (5). These protections under the third safeguard are not confined to "content", "protected material" or "protected data" but apply also to "secondary data" and to non-protected material or data.

287. The Claimant also criticises this third safeguard because it does not provide for *prior independent* authorisation of the interference. We accept the submission of Sir James Eadie that neither Strasbourg nor domestic jurisprudence lays down a general requirement for such authorisation in order to achieve compatibility with Article 8 in relation to legally privileged items: see *McE v Prison Service of Northern Ireland* [2009] UKHL 15; [2009] 1 AC 908; *RE v United Kingdom* (2016) 63 EHRR 2; *Szabo v Hungary* (2016) 63 EHRR 3; *Michaud v France* (2014) 59 EHRR 9.

288. We do not accept that the Claimant's contention is supported by the decision in *Kopp v Switzerland* (1998) 27 EHRR 91. There the Federal Prosecutor had ordered monitoring of the private and professional phone lines of a lawyer and his wife, who was the former head of the Federal Department of Justice and Police, in order to identify a person working in that Department who might have disclosed official secrets. The monitoring covered all the telephone lines in the lawyer's office and therefore also involved listening to privileged communications by all the lawyers in

the office. In those unusual circumstances, the Court expressed concern that the task of distinguishing between calls that were the subject of the investigation and other calls, the contents of which were legally privileged, had been entrusted to an official in the legal department of the Post Office without supervision by an independent judge. However, the Court did not lay down any general principle requiring prior authorisation by a judge or other independent body of the interception or obtaining of material which is the subject of legal privilege.

289. The Claimant criticises Part 7 of the 2016 Act for failing to apply the safeguards in respect of legally privileged items to "class" BPD warrants. However, we accept the Defendants' submission that such items will fall within the definition of "protected data" (section 203). In this context it should be recalled that "identifying data" which is incapable of being separated logically from BPD without revealing the meaning of any of the data is treated as "protected data". By section 202 an intelligence service may not retain, or retain and examine, BPD which includes protected data. In such circumstances, it will be necessary for a "specific" BPD warrant to be obtained and the safeguards in respect of legally privileged items will apply.

290. As for the Claimant's criticism that Chapter 2 of Part 6 does not contain specific safeguards in relation to the bulk acquisition of CD, we have previously referred to the general privacy duties in section 2 and the relevant parts of the Code of Practice. The case law upon which the Claimant relies (cited above) is all concerned with the targeted surveillance of the content of lawyer-client communications, not the obtaining or examination of CD. That case law does not lay down a lexicon of specific rules for surveillance of any lawyer-client communication. Instead, it refers to a broad principle that the importance of lawyer-client confidentiality requires specific recognition in domestic legal rules. Beyond that principle the issue of whether additional protection is required depends upon the context. That broad principle is reflected in section 2 of the 2016 Act.

291. Furthermore, as we have explained, "content" is excluded from the ambit of CD (section 261(5)). Indeed, the legislation goes further by excluding from the ambit of CD anything within the scope of "systems data" which would otherwise fall to be treated as "content". Thus, the acquisition, examination and disclosure of "content" cannot be authorised by a warrant issued under Chapter 2 of Part 6. We accept the Defendants' submission that, although CD may reveal when a communication occurred, between which devices, and for how long, it will not reveal what was discussed or the subject-matter. It will not therefore touch upon the central purpose of legal privilege, namely to enable a client to disclose whatever he wishes to in order to obtain legal advice, without the fear of that material being disclosed to others without his consent.

292. For all these reasons we are satisfied that the rules regarding legally privileged items are set out in the 2016 Act and codes of practice with sufficient clarity and with sufficient safeguards so as to avoid arbitrary interference and so as to render the statutory scheme compatible with Article 8.

The challenge in respect of confidential journalistic material

293. The Claimant contends that there are insufficient safeguards for the protection of confidential journalistic material in the 2016 Act, in particular the confidential sources of journalists. On behalf of the Claimant it is also emphasised that the considerations which apply to the importance of journalistic freedom also apply to what has been called by the Strasbourg Court "social watchdogs", in particular non-governmental organisations whose work is important to exposing action by the state, including potentially unlawful action.

294. On this ground the lead was taken at the hearing before this Court by Mr Jude Bunting, who appeared on behalf of the Intervener, the National Union of Journalists ("NUJ").

295. There is before the Court evidence as to the "chilling effect" of the broad powers contained in the 2016 Act on journalists: see the first witness statement of Ian Cobain, who is a well known investigative journalist who has worked for many years on the *Times*, then the *Guardian* and is currently with an on-line publication *Middle East Eye*. Mr Cobain expresses his concern at the impact of the powers given to the government under the 2016 Act on the ability of journalists to fulfil their functions of informing the public and exposing the truth, including state misconduct: see para. 22 of his statement.

296. The relevant scheme (both in the 2016 Act and in the Codes made under it) is summarised in the overview in the Annex to this judgment, at paras. 52-56 (bulk interception and bulk equipment interference warrants); and para. 57 (bulk acquisition warrants). Reference should also be made to the general duties in relation to privacy, which are summarised at paras. 4-6 of the overview. Section 2(2)(b) and section 2(5) are of particular importance in this context, as they emphasise the need to have regard to whether the level of protection to be applied in relation to the obtaining of information is "higher" because of the "particular sensitivity" of that information; and give, as an example, information which identifies or confirms the source of journalistic information.

297. Where a targeted warrant (for interception or examination) is sought under section 15 in Part 2 of the 2016 Act for the purposes of (among other things) examining confidential journalistic material or a journalist's source, the additional safeguards in sections 28 and 29 apply. These are linked to the arrangements which must be made under sections 53 and 150. For such targeted warrants prior approval by a Judicial Commissioner is required under section 23. The JC will have to consider the questions of necessity and proportionality: see subsection (1)(a) and (b).

298. The fundamental complaint which Mr Bunting makes is that the legal position is very different when it comes to bulk warrants under Part 6. Where information has been obtained pursuant to a bulk warrant, and one is concerned with the stage at which a decision is to be made as to whether to *examine* that information, there is no requirement for a separate or additional warrant for selection or examination, subject to the British Islands safeguard.

299. As will be apparent from the summary in the overview, there is no requirement either in the 2016 Act or in the Codes for there to be prior approval by a JC or any other independent person (that is independent of the executive) before a warrant can be

issued for the selection for examination of journalistic material or confidential journalistic material. There is a requirement to inform the IPC as soon as reasonably practicable after the event: see sections 154 and 195 of the 2016 Act. In addition, under the Codes there is a requirement to obtain the approval of a senior official who is not employed by the same agency as the analyst seeking approval.

300. The primary issue which has emerged in this context concerns whether there is a legal requirement for prior independent authorisation (not necessarily by a judicial officer). The Claimant and the NUJ submit that there is such a requirement in law. The Defendants submit that there is no such requirement.

301. The origins of the principles in this area of law are to be found in the right to freedom of expression in Article 10. It has frequently been emphasised both by the European Court of Human Rights and by domestic courts that freedom of expression is the "lifeblood" of a democratic society and that journalists in particular must be free to go about their work in order to act as "watchdogs" on behalf of the public interest. In that context Mr Bunting emphasises that the protection of journalistic sources is one of the basic conditions for freedom of the media.

302. Mr Bunting submits that the jurisprudence of the European Court of Human Rights establishes the following principles and that there is no reason why these should not apply equally where secret surveillance powers are, or may be, applied to journalists:

(1) The decision to intercept and use intercepted material should be made by a judge or another independent and impartial decision-making body. The body must be separate from the executive and other interested parties. He relies in particular on the decisions of the European Court of Human Rights in *Sanoma Uitgevers BV v Netherlands* [2011] EMLR 4; *Telegraaf Media Nederland Landelijke Media BV v Netherlands* (Application No 39315/06, judgment of Third Section, 22 November 2012); and *Nagla v Latvia* (Application No 72469/10, judgment of Fourth Section, 16 July 2013). He also relies on the decision of the Court of Appeal in *R (Miranda) v Secretary of State for the Home Department* [2016] EWCA Civ 6; [2016] 1 WLR 1505.

(2) This independent decision must take place before interception occurs or (if it occurs urgently) before any use is made of the intercepted material; and the reviewing body must have the power to prevent interception or use of it. This is because the exercise of any independent review which only takes place subsequently to the handing over of material capable of revealing the journalist's confidential source would undermine the very essence of the right to confidentiality.

(3) There must be an overriding public interest to justify such interception and use of the intercepted materials. The independent body must therefore be invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the source's identity if it does not; and it must be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material which it is sought to have disclosed

so that the arguments of the authorities seeking disclosure can be properly assessed.

(4) The decision to be taken should be governed by clear criteria, including whether a less intrusive measure would suffice to serve the overriding public interest established. The independent body must have power to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material.

303. Further, Mr Bunting submits that, even if this Court is persuaded that it is permissible in principle to obtain information on a bulk scale, the principles established in Strasbourg make it clear that there is a need for independent authorisation where:

(1) The state has an intention of selecting, examining, or searching material to identify a journalistic source or to obtain journalistic materials.

(2) State searches are likely to, or even simply "could", reveal the identity of a source or journalistic material.

(3) It is realised that material being examined is journalistic material.

304. On behalf of the Defendants Sir James Eadie submits that the "core answer" to the NUJ's complaint is that it has misunderstood the effect of the caselaw of the European Court of Human Rights and also the decision of the Court of Appeal in *Miranda*. He submits that that jurisprudence requires prior independent authorisation (save in urgent cases) only where an *order* is sought requiring the divulging of a journalistic source, or where the purpose of *obtaining* material in the first place is to discover a journalistic source; not at the stage of *selection for examination* of material that has already been obtained under bulk powers.

305. Further, Sir James Eadie submits that the suggested requirement of prior independent authorisation is plainly inconsistent with the decisions in *Weber and Saravia* and *Big Brother Watch*. He submits that those decisions explicitly indicate that such independent authorisation is not required where information is obtained in bulk and is then searched in order to identify a source or to obtain journalistic material (let alone where that is simply one possible consequence of the search).

306. Sir James Eadie also observes that submissions very similar to the ones made on behalf of the NUJ in the present case were made on its behalf in the first section in *BBW* in which the NUJ had also intervened. At the hearing we were informed that the NUJ has not intervened in the proceedings before the Grand Chamber although there is a similar organisation (the Bureau of Investigative Journalists) which is one of the applicants before that Court.

307. The starting point for our analysis is the decision in *Miranda*. This is because this is a decision of the Court of Appeal and its *ratio* is therefore binding on this Court. So far as relevant that case was concerned with the potential impact on journalistic freedom of the power to stop a person at an airport under para. 2(1) of Sch. 7 to the Terrorism Act 2000 ("the 2000 Act"). In reversing the Divisional Court on this aspect of the case only, the Court of Appeal made a declaration (under section 4 of the HRA) that the

stop power in that provision was incompatible with Article 10 of the Convention in relation to journalistic material in that it was not subject to adequate safeguards against its arbitrary exercise. The Court said that it would then be a matter for Parliament to provide such protection but the most obvious safeguard would be some form of judicial or other independent and impartial scrutiny conducted in such a way as to protect the confidentiality in the material: see para. 119 in the judgment of Lord Dyson MR (with whose judgment the other members of the Court agreed).

308. Lord Dyson considered the issue of compatibility with Article 10 at paras. 94-117 of his judgment. At para. 101 he said:

> "It is clear enough that the Strasbourg jurisprudence requires prior, or (in an urgent case) immediate post factum, judicial oversight of interferences with Article 10 rights where journalists are required to reveal their sources. In such cases, lack of such oversight means that there are no safeguards sufficient to make the interference with the right 'prescribed by law'. This is not surprising in view of the importance to press freedom of the protection of journalistic sources …"

309. At para. 102 Lord Dyson noted that the case before the Court was not about disclosure of a journalist's source since that source was already known. The question which therefore arose was whether prior or (in an urgent case) immediate *post factum* judicial authorisation is required as an adequate safeguard before journalistic material can be obtained in a case where the identity of the source is known. Having referred to the relevant Strasbourg authorities, including many of those which have been referred to this Court (including *Sanoma, Telegraaf* and *Nagla*) Lord Dyson concluded that the 2000 Act did not contain adequate safeguards against arbitrary decision-making. At para. 113 he said:

> "… the central concern is that disclosure of journalistic material (whether or not it involves the identification of a journalist's source) undermines the confidentiality that is inherent in such material and which is necessary to avoid the chilling effect of disclosure and to protect Article 10 rights. If journalists and their sources can have no expectation of confidentiality, they may decide against providing information on sensitive matters of public interest. That is why the confidentiality of such information is so important. It is, therefore, of little or no relevance that the Schedule 7 powers may only be exercised in a confined geographical area or that a person may not be detained for longer than nine hours. I accept that the fact that the powers must be exercised rationally, proportionately and in good faith provides a degree of protection. But the only safeguard against the powers not being so exercised is the possibility of judicial review proceedings. In my view, the possibility of such proceedings provides little protection against the damage that is done if journalistic material is disclosed and used in circumstances where this should not happen. An important rationale for the principle of legal certainty that underpins the concept of 'prescribed by law' is that there should be

> *adequate* safeguards against arbitrary decision-making. Unlike the position in relation to Article 5 and 9, the possibility of judicial review proceedings to challenge the rationality, proportionality and good faith of a decision to interfere with freedom of expression in cases involving journalistic material cases does not afford an adequate safeguard." (Emphasis in original)

310. At para. 114 Lord Dyson continued that:

> "Laws LJ may be right in saying that the European Court of Human Rights has not developed an 'absolute' rule of judicial scrutiny for cases involving state interference with journalistic freedom. But prior judicial or other independent and impartial oversight (or immediate post factum oversight in urgent cases) is the natural and obvious adequate safeguard against the unlawful exercise of the Schedule 7 powers in cases involving journalistic freedom. …"

311. At paras. 115-116 Lord Dyson contrasted the provisions of the 2000 Act with the provisions of other legal regimes, which he described as "striking". For example, section 9 of, and Sch. 1 to, the Police and Criminal Evidence Act 1984 ("PACE") governs the grant by a court of a production order. In that context "journalistic material" falls within the categories of "special procedure material" or "excluded material" as defined in sections 11-14 of PACE. Such material is afforded additional protections, such that access can only be gained on an *inter partes* application before a Circuit Judge, in which the stringent requirements of Sch. 1 must be met. Sch. 5 to the 2000 Act itself empowers a court (again following an *inter partes* hearing) to order the seizure or production or special procedure and excluded material for the purpose of a terrorist investigation provided the statutory criteria are satisfied.

312. In the present context, our attention was drawn to section 77 of the 2016 Act, which does require the approval of a Judicial Commissioner in circumstances where a designated senior officer has granted an authorisation in relation to the obtaining by a relevant public authority of communications data for the purpose of identifying or confirming a source of journalistic information and the authorisation is not necessary because of an imminent threat to life.

313. What the existence of such provisions elsewhere in domestic legislation does not, however, demonstrate is that there is any requirement *in the ECHR* for there to be such prior judicial or other independent authorisation. It is exclusively that question of Convention law with which this Court is presently concerned.

314. In our view, the decision in *Miranda* is distinguishable from the present context for the reasons that Sir James Eadie has advanced on behalf of the Defendants. In essence that case concerned the compulsory seizure of journalistic material pursuant to the power to stop, question and detain a person at an airport in para. 2(1) of Sch. 7 to the 2000 Act. In the present context the issue does not arise from the initial compulsory

obtaining of the relevant material but rather with the later stage of its selection for examination. We therefore turn to the Strasbourg caselaw.

315. The first case which must be considered is *Weber and Saravia*. It is important to note that this was a case about "strategic surveillance". It is also important to note that in that case the first applicant was herself a journalist. Furthermore, one of the grounds of complaint made to the European Court of Human Rights arose under Article 10: see paras. 139-153 of the Court's judgment. The Court concluded that the first applicant's complaints under Article 10 were "manifestly ill-founded", and for that reason inadmissible.

316. In the course of its reasoning, the Court addressed the question whether there was an interference with the applicant's rights under Article 10, at paras. 143-146, and concluded that there was. In particular, the Court again reiterated that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. Further, the protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result the vital "public watchdog" role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be adversely affected. The Court observed that the applicant had communicated with persons she wished to interview on subjects such as drugs and arms trafficking or preparations for war. Consequently, there was a danger that her telecommunications for journalistic purposes might be monitored and that her journalistic sources might be either disclosed or deterred from calling or providing information by telephone. The failure to notify the first applicant of surveillance measures could serve to impair the confidentiality and protection of information given to her by her sources.

317. The Court then considered whether the interference with the applicant's right to freedom of expression was "prescribed by law" and concluded that it was: see para. 147. In para. 152 the Court noted that the legislation did not contain special safeguards for protecting press freedom, and in particular the non-disclosure of sources, once the authorities became aware that they had intercepted a journalist's conversation. Nevertheless, the Court decided that the general safeguards in the legislation were adequate for the purposes of Article 10. It relied on its earlier reasoning at paras. 93-102 as to why any interference with Article 8 rights was "in accordance with the law": in that earlier passage the Court had concluded that the interferences with the applicants' right to respect for private life and correspondence were in accordance with the law.

318. In the *Telegraaf* case the Court considered its earlier decision in *Weber and Saravia* in the context of its discussion of the question whether the interference with Article 8 and Article 10 rights in that case was in accordance with the law/prescribed by law, at paras. 89-102. The Court concluded that the law in that case did not provide adequate safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources. However, it is important to appreciate the reasoning of the Court and why it distinguished *Weber and Saravia*. At paras. 96-97 the Court said:

> "96. In *Weber and Saravia*, the interference with the applicants' rights under Articles 8 and 10 consisted of the interception of telecommunications in order to identify and avert dangers in advance, or 'strategic monitoring' as it is also called. The first applicant in that case being a journalist, the Court found that her right to protect her journalistic sources was in issue … However, the aim of strategic monitoring was not to identify journalists' sources. Generally the authorities would know only when examining the intercepted telecommunications if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring could not, therefore, be characterised as particularly serious … Although admittedly there was no special provision for the protection of freedom of the press and, in particular, the non-disclosure of sources once the authorities had become aware that they had intercepted a journalist's conversation, the safeguards in place, which had been found to satisfy the requirements of Article 8, were considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum …
>
> 97. The present case is characterised precisely by the targeted surveillance of journalists in order to determine from whence they have obtained their information. It is therefore not possible to apply the same reasoning as in *Weber and Saravia*."

319. At paras. 98-102 the Court then proceeded to apply the principles which it had developed in earlier decisions such as *Klass v Germany* (1979-80) 2 EHRR 214 and *Sanoma*. It concluded that, in the circumstances, prior independent authorisation was required.

320. It will be seen therefore that the basis on which the Court distinguished *Weber and Saravia* was that the surveillance measures were themselves "targeted", in particular they were directed at uncovering journalistic sources. Had that not been the case, the case would have been identical to the case of *Weber and Saravia*, and the absence of any special provision for the protection of freedom of the press at the stage when the authorities become aware that they had intercepted a journalist's conversation would not have been material, provided sufficient safeguards were in place so as to satisfy the requirements of Article 8. In particular, there is no suggestion in the reasoning in either *Weber and Saravia* or *Telegraaf* that prior judicial or other independent authorisation is required in circumstances where material has been obtained and only later is it to be examined in order to see (for example) who the source of a journalist's information was. There still have to be sufficient safeguards against the risk of abuse of a discretionary power. It does not follow that those safeguards must include prior judicial or other independent authorisation.

321. It seems to us that the decision of the European Court of Human Rights in *Sanoma* is also distinguishable from the present context because, as Sir James Eadie has submitted, it too concerned orders to disclose sources: see para. 89 of the judgment.

That is how the decision was understood by the Court in its later judgment in *Telegraaf*, at para. 99. We note that in *Sanoma* there had in fact been an investigating judge but the criticism which the European Court eventually made related to the limited powers of that judge: it was not open to that judge to issue, reject or allow a request for an order, or to qualify or limit such an order as appropriate. His role was what could only be described as "an advisory role": see para. 97 of the judgment. Accordingly, the quality of the law in that case was deficient in that there was no procedure attended by adequate legal safeguards for the applicant company in order to enable an independent assessment as to whether the interest of the criminal investigation overrode the public interest in the protection of journalistic sources: see para. 100.

322. We have come to the view that the decision of the European Court in *Nagla v Latvia* is also distinguishable from the present context because it concerned a search at the applicant's home. In the result the Court in fact concluded that the interference in that case was prescribed by law: see para. 91 of its judgment. Although the case does concern journalistic material, it is, in our view, a long way from the present sort of context, which concerns secret surveillance and, in particular, bulk powers leading to a later selection for examination of journalistic material.

323. That then brings us to the recent and important decision of the First Section of the European Court of Human Rights in *Big Brother Watch*. This is important not least because it is one of the few cases in Strasbourg (like *Weber and Saravia*) which has expressly considered the issue of journalistic freedom in the context of secret surveillance measures.

324. In *Big Brother Watch* the Court considered Article 10 at paras. 469-500 of its judgment. At para. 485 the Court recorded that the NUJ was among the interveners in that case and submitted that the confidentiality of sources was indispensable for press freedom. It also expressed concern about the possible sharing of data by the UK with other countries. At the hearing before this Court we were provided by the Defendants with the written submissions which were made by interveners in that case, including the NUJ. In those written submissions, which were not drafted by Mr Bunting, the interveners submitted, at paras. 28-35, that there were certain necessary safeguards which had to be contained in a legislative scheme for the bulk collection of data which might have an impact on journalistic freedom. In particular, at para. 31, it was submitted that, where the state had enacted broad powers to obtain external communications and metadata which could identify confidential sources and provide access to other confidential material, without the journalist or the source ever having any notice of the interception, the safeguards should be either (a) prior judicial, or at least independent, control of access to external communications and/or metadata (it was pointed out that *post factum* control may not be sufficient to prevent disclosure of the information); or (b) in urgent cases, at the very least judicial or independent control post-interception but before the content or data is accessed or analysed. Sir James Eadie observes that that is in substance the submission which Mr Bunting has advanced on behalf of the NUJ in the present case also.

325. In its judgment in *Big Brother Watch* the Court noted, at para. 486, the intervention of the Media Lawyers' Association, which expressed deep concern that domestic law was moving away from the strong presumption that journalistic sources would be afforded special legal protection, since surveillance regimes allowed the authorities to

intercept journalists' communications without the need for prior judicial authorisation. It is clear therefore, in our view, that the issue was squarely before the First Section. The Court then addressed the issue so far as relevant at paras. 487-500.

326. It set out general principles first, at paras. 487-489. It considered its earlier decisions, including *Weber and Saravia* and *Sanoma*. At para. 489 the Court said:

> "The Court has recognised that there is 'a fundamental difference' between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources … The Court considers that the latter, even if unproductive, constituted a more drastic measure than an order to divulge the source's identity, since investigators who raid a journalist's workplace have access to all documentation held by the journalist … However, the Court has also drawn a distinction between searches carried out on journalists' homes and workplaces 'with a view to uncovering their sources', and searches carried out for other reasons, such as the obtaining of evidence of an offence committed by a person other than in his or her capacity as a journalist … Similarly, in *Weber and Saravia*, the only case in which the Court has considered, in abstracto, the Article 10 compliance of a secret surveillance regime on account of the potential for interference with confidential journalistic material, it considered it decisive that the surveillance measures were not aimed monitoring journalists or uncovering journalistic sources. As such it found that the interference with freedom of expression could not be characterised as particularly serious …"

327. The Court then considered in turn first the section 8(4) of RIPA regime and, secondly the regime in Chapter II of RIPA.

328. At para. 492, the Court again observed that the surveillance measures under the section 8(4) regime (like those under the G10 Act which were considered in *Weber and Saravia*) were "not aimed at monitoring journalists or uncovering journalistic sources". The Court continued:

> "… Generally the authorities would only know when examining the intercepted communications if a journalist's communications had been intercepted. Consequently, it confirms that the interception of such communications could not by itself, be characterised as a particularly serious interference with freedom of expression … However, the interference will be greater should these communications be selected for examination and, in the Court's view, will only be 'justified by an overriding requirement in the public interest' if accompanied by sufficient safeguards relating both to the circumstances in which they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination."

329. In that regard the Court observed, at para. 493, that it was:

> "of particular concern that there are no requirements – at least, no 'above the waterline' requirements – either circumscribing the intelligence services' power to search for confidential or other material (for example by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or maybe involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications."

330. Safeguards did exist in respect of the storing of confidential material once identified: see para. 494.

331. The Court concluded its assessment of the section 8(4) regime in the following way, at para. 495:

> "Nevertheless, in view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any 'above the waterline' arrangements limiting the intelligence services' ability to search and examine such material other than where 'it is justified by an overriding requirement in the public interest', the Court finds that there has also been a violation of Article 10 of the Convention."

332. The Court addressed the Chapter II regime at paras. 496-499 of its judgment. This related to the acquisition of communications data from communication service providers. The Court cross-referred back to para. 467 of its judgment, where it had already concluded that the Chapter II regime was not in accordance with the law as it permitted access to retained data for the purpose of combatting crime (rather than "serious crime") and, save for where access was sought for the purpose of determining a journalist's source, it was not subject to prior review by a court or independent administrative body. That was a reference to this Court's judgment of 27 April 2018 in the context of the challenge to the 2016 Act under EU law: see [2019] QB 481. Since EU law is for this purpose part of domestic law, the requirement that there must be compliance with domestic law in order for there to be compliance with the Convention requirement of law was clearly not met.

333. Nevertheless, Mr Bunting is entitled to observe that the Court did not stop there. It continued, at para. 498, to consider the requirements of the acquisition of communications data code, particularly para. 3.77; and also applications for a production order under PACE. Nevertheless, the Court concluded, at para. 499, as follows:

> "… These provisions only apply where the purpose of the application is to determine a source; they do not, therefore, apply in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely. Furthermore, in cases concerning access to a journalist's communications data there are no special provisions restricting access to the purpose of combatting 'serious crime'. Consequently, the Court considers that the regime cannot be 'in accordance with the law' for the purpose of the Article 10 complaint."

334. In our view, Sir James Eadie is correct to submit that it would have been very easy for the First Section simply to state that, in this context, there is a requirement for judicial or other independent prior authorisation before selection for examination of journalistic material may occur after bulk data has been collected. The Court was faced with submissions precisely inviting it to say so. The Court declined that invitation. What the Court required was that there should be "sufficient safeguards". We also accept the submission made by Sir James Eadie that the primary basis for why the Court concluded that there was a breach of the requirement of law in respect of the Chapter II regime was that there was a breach of domestic law (for this purpose including EU law).

335. We do not consider that the present context is an appropriate one in which this Court should go further than the Strasbourg Court has to date been prepared to go. This is in accordance with the well known principle enunciated by the House of Lords ever since 2004 that domestic courts, although not bound by the decisions of the European Court of Human Rights by virtue of the provisions of section 2 of the HRA, should keep pace with the clear and constant jurisprudence of the European Court of Human Rights but no more or less. In *R (Ullah) v Special Adjudicator* [2004] UKHL 26, [2004] 2 AC 323, Lord Bingham of Cornhill stated, at para. 20, that:

> "… It is of course open to member states to provide for rights more generous than those guaranteed by the Convention, but such provision should not be the product of interpretation of the Convention by national courts, since the meaning of the Convention should be uniform throughout the states party to it. The duty of national courts is to keep pace with the Strasbourg jurisprudence as it evolves over time: no more, but certainly no less."

336. In *R (Al-Skeini and others) v Secretary of State for Defence* [2007] UKHL 26, [2008] 1 AC 153, after quoting the above passage, Lord Brown of Eaton-under-Heywood stated, at para. 106:

> "I would respectfully suggest that last sentence could as well have ended: 'no less, but certainly no more.' There seems to me, indeed, a greater danger in the national court construing the Convention too generously in favour of an applicant than in construing it too narrowly. In the former event the mistake will necessarily stand: the

> member state cannot itself go to Strasbourg to have it corrected; in the latter event, however, where Convention rights have been denied by too narrow a construction, the aggrieved individual *can* have the decision corrected in Strasbourg". (Emphasis in original)

337. We certainly see the force of the submissions which were attractively made by Mr Bunting and it may well be that the "direction of travel" is favourable to his case. Nevertheless, we have reached the conclusion that the provisions of the 2016 Act are not incompatible with Article 10 of the ECHR in so far as it is suggested that there are inadequate protections for journalistic material. Mr Bunting's submissions would require this Court to go where the Strasbourg Court has (to date) not itself been prepared to go. We consider that it would not be appropriate to anticipate what the Grand Chamber may say about this in *Big Brother Watch*.

338. In the skeleton argument filed on behalf of the NUJ Mr Bunting raised some other matters that were not developed at the oral hearing before this Court. We will therefore deal with them relatively briefly.

339. At paras. 39-41 of the NUJ's skeleton, Mr Bunting argues that section 264(2) of the 2016 Act defines "journalistic material" too narrowly. He sets out five separate bases for this complaint.

340. The first is that the section 264(2) definition stretching to "material created or acquired *for the purposes of journalism*" (emphasis added) is too narrow since the Convention provides protection to all "documentation held by [a] journalist", irrespective of whether it is directly held for the purposes of journalism. Much of the material provided to journalists will not necessarily become part of a story, so the additional purposive element is too restrictive. For this purpose Mr Bunting cites *Telegraaf*, at para. 86; and *Sanoma*, at paras. 67 and 72.

341. We do not accept that this is what the Court was saying in *Sanoma*. The Court uses the quoted phrase as part of explanation as to why an order for search and seizure in a journalist's workplace was more intrusive than an order to divulge the source's identity, given that the former gave access "to all the documentation held by the journalist". The full paragraph reads as follows:

> "In earlier case-law the Court has considered the extent to which the acts of compulsion resulted in the actual disclosure or prosecution of journalistic sources irrelevant for the purposes of determining whether there has been an interference with the right of journalists to protect them. In the case of *Roemen and Schmit*, the information sought was not obtained as a result of the execution of the order for search and seizure in the journalist's workplace. This order was considered 'a more drastic measure than an order to divulge the source's identity ... because investigators who raid a journalist's workplace unannounced and armed with search warrants have very wide investigative powers, as, by definition, they have access to all the documentation held by the journalist. It thus considers that the searches of the first applicant's

> home and workplace undermined the protection of sources to an even greater extent than the measures in issue in *Goodwin*' (loc. cit., § 57)."

342. Moreover, the citation from *Telegraaf* does not provide the support that Mr Bunting considers it does. At para. 86, the European Court of Human Rights states that it "understands 'information identifying a source' to include, as far as they are likely to lead to the identification of a source, both 'the factual circumstances of acquiring information from a source by a journalist' and 'the unpublished content of the information provided by a source to a journalist'". It does not state that *any* documentation held by a journalist is protected, and indeed such a position would be unworkable, applying to any interchange between a journalist and anyone else at all.

343. The 2016 Act's definition (with its reference to the "purposes of journalism") is sufficiently broadly-worded to cover the material protected by the Convention as stated in *Telegraaf*, as conceivably material "provided by a source to a journalist" will be held for "the purposes of journalism". If the wording of the Act does not cover this material on its face, then it can be read in that way pursuant to the strong interpretative obligation in section 3 of the HRA (to which we have referred earlier in this judgment).

344. If the definition does so extend, then the Act will meet the "foreseeability" requirement in that it will be relatively clear when material has been provided by a source to a journalist, and, more generally, when it is being held for the purposes of journalism.

345. The second basis of complaint is that the 2016 Act's definition wrongly requires an "express or implied undertaking" to hold material in confidence. We do not consider that this Court has been shown any authority which throws the compatibility of this part of the Act's definition into question. Mr Bunting relies again on *Sanoma*, at para. 64, where the European Court of Human Rights said:

> "the Court is of the view that although the question has been the subject of much debate between the parties, it is not necessary to determine whether there actually existed an agreement binding the applicant company to confidentiality. The Court agrees with the applicant company that *there is no need to require evidence of the existence of a confidentiality agreement beyond their claim that such an agreement existed*." (Emphasis added)

346. In that passage the Court was dealing with an evidential point concerning the existence of a confidentiality agreement on the facts of that particular case. It stops far short of holding that the requirement of an "express or implied undertaking" of confidentiality is contrary to the Convention. Furthermore, the intelligence services can fairly assume that material held by a journalist which has come from a source is held according to such an undertaking, and so there is no incompatibility with the Convention concept of "law" arising from this.

347. In any event, the Act's reference to "an express or implied undertaking of confidentiality" is broad, comprehending all the circumstances in which an obligation

of confidence may arise at law or in equity. This is a very broad category that would readily apply to many situations in which journalists exchange information. It therefore does not unduly restrict the definition of "journalistic material" in the way contended.

348. The third complaint is that it is unclear to what extent the 2016 Act's definitions will apply to the new generation of journalists who publish material on blogs or on social media. We do not think that this complaint is well-founded. Mr Bunting criticises the "relevant factors" within the GCHQ Compliance Guide and in the related codes of practice, suggesting that factors like "whether they receive remuneration for their work", the "frequency of the individual's relevant activities", the "means by which they disseminate that information", and "the level of personal rigour they seek to apply to their work" might be difficult for bloggers to meet. Only the first of these factors might in reality be problematic for "blogger" journalists, and these factors are plainly intended to be indicative factors rather than statutory requirements. Blogger journalists can readily be caught by the definition.

349. Furthermore, as Sir James Eadie submitted at the hearing, there will be matters such as the definition of a "journalist" which may well develop in particular cases which are decided by the courts in the future. To what extent, for example, that concept includes someone who is a "blogger" on the internet may well be the subject of future judicial decision. None of that, in our view, leads to the conclusion that the 2016 Act is incompatible with the Convention rights as alleged.

350. The fourth basis on which Mr Bunting complains about the definition of journalistic material is the same as that outlined by the Claimant, at paras. 176-177 of its skeleton. Both the Claimant and the NUJ emphasise that Article 10 requires that special "journalistic" protections are accorded also to "social watchdog" organisations such as Liberty itself: see e.g. *Társaság a Szabadságjogokért v Hungary* (2011) 53 EHRR 3; and *Magyar Helsinki Bizottság v Hungary* (Application No 18030/11, Grand Chamber, judgment of 8 November 2016), yet neither the IPA nor the codes of practice make reference to such organisations.

351. In our view, what is required under Article 10 is not that such types of organisations are expressly mentioned, but that those organisations are sufficiently protected by the 2016 Act and codes in order to meet the requirements of Article 10. In this judgment we have sought to set out why the safeguards framed within the Act and Codes comply with the current Strasbourg jurisprudence on Article 10 in relation to journalists: those protections apply *mutatis mutandis* to watchdog organisations such as the Claimant.

352. The fifth complaint is that the exclusion of certain material from "journalistic material" because it was "created … with the intention of furthering a criminal purpose" in section 264(5) goes too far in excluding material which ought to be protected. Mr Bunting did not cite any Strasbourg authority which suggests that this inclusion is problematic, nor do we think that the inclusion creates any difficulty with the compatibility of the definition taken as a whole with the Convention rights.

MI5's handling arrangements

353. A new issue has emerged over the last few months which is alleged by the Claimant to undermine the safety of the safeguards which are said to be in place as a result of the 2016 Act. On behalf of the Claimant Mr Jaffey took the lead in making submissions on this issue.

354. The issue arises from recent disclosure made by the Defendants pursuant to their duty of candour and co-operation with the Court, in relation to defects which have been identified in the handling arrangements on the part of MI5.

355. As we have mentioned earlier, there is before the Court an application by the Defendants to hold a CMP under section 6 of the Justice and Security Act 2013. This has been made out of an abundance of caution. There is nothing which the Defendants themselves wish the Court to take into account on the substantive issues which would require a CMP to be adopted. On the other hand, in order to fulfil their duties to the Court, the Defendants have (by way of precaution) made that application in case the Court should consider it to be necessary. For their part the Claimant's representatives have now been provided with a considerable amount of disclosed material (redacted where necessary). This has been the result in part of voluntary disclosure and otherwise the product of discussions which have taken place between the Defendants' representatives and Special Advocates (led by Mr Angus McCullough QC). We are grateful to all those concerned for their co-operative attitude and the assistance which they have provided to the Court. The net result has been that Mr Jaffey was able to make the submissions which he wished to on the basis of the documents which have been disclosed. The redactions in them have not hampered his ability to make the submissions which he wished to. It was clear to the Court that it was not necessary for a CMP to be used in this case in order to adjudicate fairly on the issues in the case. Nevertheless, very fairly, the Defendants have maintained the application under section 6 in place because they recognise that their duties to the Court are of a continuing nature.

356. Pursuant to that continuing duty, after the hearing in this case, the Defendants disclosed a summary of the report by Sir Martin Donnelly, who conducted a Compliance Improvement Review at the request of the Home Secretary. The summary and recommendations of the Review were published on 15 July 2019, with redactions for national security reasons. The Claimant asked for, and was given, a short time to make brief written submissions about this. The Defendants were given a short time to respond. The NUJ did not wish to make submissions about this issue. We are grateful to the parties for their submissions, which we have taken into account before finalising this judgment. The Defendants have indicated that they will continue to keep their obligations of candour and co-operation under review, and will in due course disclose the full report of the Compliance Improvement Review and any further report by the IPC (subject to redactions on national security grounds and after discussion with the Special Advocates). The parties were agreed in their recent written submissions that there was no need for the Court to delay handing down its judgment to await these developments but were content to leave that question for the Court to determine. For reasons that will become apparent later, we do not consider that it is necessary to delay handing down our judgment, in the light of the conclusion that we have reached on this issue on the basis of the documents that have been placed before us, including the post-hearing disclosure.

357. We turn to the substance of the argument which the Claimant makes based on the recently disclosed material. The essential submissions which Mr Jaffey makes in this context are as follows:

(1) The caselaw on the ECHR makes it clear that not only must there be sufficient safeguards in place against the risk of abuse of discretionary powers in the sensitive area of secret surveillance, those safeguards must be effective in practice rather than merely theoretical.

(2) The recent disclosure shows that there have for several years been serious failures on the part of MI5 in relation to its handling arrangements, particularly in respect of the retention of data collected pursuant to warrants. These failures have caused such concern to the IPC that he has described MI5 as being in effect in "special measures."

(3) In consequence, the Court cannot be satisfied that the arrangements for safeguarding material obtained under the 2016 Act are effective in practice and therefore the Court should make a declaration of incompatibility in respect of that Act, in particular the safeguards relating to retention, examination, use, destruction and oversight.

358. The Claimant reminds the Court that the core of the statutory protection for privacy over warranted data once obtained is provided by the retention safeguards provisions in the 2016 Act: see in particular section 53 (targeted and thematic interception); section 129 (targeted and thematic equipment interference); section 150(2), and (4)-(5) (bulk interception); section 171 (bulk communications data); and section 191(2) and (4)-(5) (bulk equipment interference).

359. The Claimant submits that the basic principles in the 2016 Act are clear. Arrangements must be in place to ensure that:

(1) the number of persons, extent of any disclosure, extent of any copying and number of copies made are kept to the minimum necessary;

(2) the material must be stored in a secure manner; and

(3) each copy made of any material or data must be destroyed as soon as its retention is no longer necessary.

The effect is said to be that, subject to the power to retain data under Part 7, it is usually only retained for a short period and then permanently deleted.

360. Further, under the 2016 Act, warrants cannot be lawfully granted unless proper arrangements are in place. The Secretary of State must be satisfied that the product of warrants will be appropriately safeguarded; otherwise the application for a warrant cannot be granted. The same approach would have to be taken by a JC when asked to approve the grant of a warrant.

361. It is unnecessary to set out in full here the documents which have recently been disclosed in relation to MI5's handling arrangements for the retention of data. A flavour of those documents can be obtained from the following:

(1) A letter from MI5's Director of Policy, Compliance, Security and Information to the IPC dated 11 March 2019, which summarised a briefing which had been given by MI5 to the IPC on 27 February 2019. That was the first time, it appears, that the IPC was made aware of the problems which have been identified on the part of MI5.

(2) The IPC's first inspection report issued on 29 March 2019.

(3) A new Annex H – Section II to the MI5 Handbook for Judicial Commissioners issued on 1 April 2019.

(4) The Generic Decision on warrants by the IPC dated 5 April 2019.

(5) A letter from Sir Andrew Parker, Director General of MI5, to the Home Secretary dated 24 April 2019 and a letter from Sir Andrew Parker to the IPC dated 26 April 2019.

(6) The IPC's second inspection report of MI5 dated 26 April 2019.

362. At para. 10 of the Generic Decision the IPC summarised the nature of the problem as that MI5 had "inadequate control over where data is stored; [REDACTED]; and the deletion processes which applied to it." Specific areas identified by the IPC included the absence of proper mechanisms for review, retention and destruction of retained data, specifically an absence of effective safeguards relating to material which was subject to legal professional privilege. Furthermore, the letter from MI5 dated 11 March 2019 revealed that an MI5 compliance team had identified as early as January 2016 that "data might be being held in ungoverned spaces in contravention to our policies". Mitigation work was sought in early 2018.

363. The Generic Decision notes that warrants were issued to MI5 on a basis that MI5 knew to be incorrect and that consequently JCs were given false information. The IPC noted in that decision that by January 2018 at the latest, the Management Board at MI5 had a clear view of serious problems with the manner in which warranted data is held in the "technology environment" ("TE"). There was a real possibility that the destruction of material was not being implemented appropriately. The IPC was of the view that, even by the time of the briefing given to him on 27 February 2019, MI5 continued to use a "misleading euphemism" of "compliance difficulties". In his Generic Decision the IPC said:

> "46. … I do not intend in this Decision to set out the precise nature of the inspection regime and the various forms of monitoring that will need to take place, but I want there to be no doubt as to the gravity of the situation and the need for IPCO to be reassured that breaches of the legislation are not ongoing. This will involve frequent inspections by IPCO, beginning on 15 April 2019, and I expect the inspectors to be afforded direct access to members of staff. It will be unacceptable for the inspectors to be asked to rely on hearsay accounts of internal conversations between members of MI5. I am confident that a method of undertaking this form of inspection can be secured without causing undue anxiety for members of MI5. …

> 49. This is a serious and inherently fragile situation. The future will entirely depend on compliance by MI5 with the legislation and the adequacy of the internal and external inspection regimes. IPCO will need to be reassured on a continuing basis that new warranted material is being handled lawfully. In the absence of this reassurance, it is likely that future warrant applications for data held in [TE] will not be approved by the Judicial Commissioners, and I will expect that the proposed mitigations are progressed at pace. The weaknesses outlined above are of sufficient magnitude to mean that the immediate mitigatory steps, which will be sufficient for the short term, cannot be expected to provide a long term solution, and the proposals made by MI5 in part II must be implemented in their entirety in the shortest reasonable timeframe. Without seeking to be emotive, I consider that MI5's use of warranted data in [TE] is currently, in effect, in 'special measures' and the historical lack of compliance with the law is of such gravity that IPCO will need to be satisfied to a greater degree than usual that it is 'fit for purpose'. It is of importance to add by way of postscript that now this problem has been ventilated, MI5 appear to be using every endeavour to correct the failings of the past and to secure compliance. The organisation has cooperated in every way with the inspection we recently conducted and the questions that I posed."

364. Earlier in the Generic Decision, at paras. 44-45, it was said:

> "44. Albeit not strictly relevant to the present application, it is clear that for warranted material in [TE] there has been an unquantifiable but serious failure to handle warranted data in compliance with the IPA for a considerable period of time, and probably since IPCO first became operational. Assurances that have been made to the Secretary of State and the Judicial Commissioners of such compliance were, in hindsight, wrong and should never have been made. Warrants have been granted and judicially approved on an incomplete understanding of the true factual position. Indeed, I am concerned that on this important subject we were incompletely briefed during the Commissioners' induction programme, including that most recently provided to Lord Hughes and Sir Colman Treacy. To date, therefore, MI5's retention of the warranted material in [TE] cannot be shown to have been held lawfully and the failure to report these matters timeously to IPCO is a matter of grave concern which I will be addressing separately. The critical question, however, on this application is whether the data to be covered by the present warrant will be appropriately safeguarded.
>
> 45. On the basis of the mitigations set out in Section II, combined with the answers to the questions that I have received, subject to certain critical caveats, I am satisfied that MI5 have the capability henceforth to handle warranted data in a way which is compliant with the IPA. … The key caveat is that all the relevant activities must be

> susceptible to inspection and audit – in other words, MI5 and IPCO must be able to check in sufficient detail that there has been compliance with the legislation."

365. In the first inspection report by the IPC dated 29 March 2019, at para. 5 there was consideration of material subject to legal privilege. At para. 5.1.4 it was said:

> "In addition, [REDACTED], it is unlikely MI5 could give complete assurance it had complied with any conditions imposed by a JC as to the use or retention of legally privileged items."

366. Before this Court Mr Jaffey has taken us to a number of documents which have been disclosed by the Defendants which set out in tabular form a risk rating, showing red, amber and green ratings for various compliance risks. A red rating indicates "serious compliance gaps"; and an amber rating indicates "some compliance gaps." Some of those entries are redacted. Nevertheless, Mr Jaffey submits that it is apparent that on any view there are serious risks mentioned, including in relation to compliance with the 2016 Act.

367. Furthermore, after a letter was sent by MI5 on 3 May 2019, the IPC replied in a letter dated 8 May 2019. In that letter the IPC noted that there were further errors. First, it appeared that MI5 had been aware of a compliance risk in "[area 1]" and "[area 2]" since 2016. The IPC expressed his concern that this information was not included in either the original briefing to him on 27 February 2019 or the letter dated 11 March 2019. Secondly, to the extent that [area 1] or [area 2] contained warranted data, it would be helpful for the IPC to understand whether MI5's use of either area is in breach of the 2016 Act's safeguards. He said:

> "From the limited information so far provided it seems highly likely that this is the case, but I would welcome the earliest information on this point from MI5's perspective. If that assumption is correct, this raises the question as to whether MI5 has the capability to handle warranted data in an IPA-compliant fashion."

368. MI5 replied in a letter dated 15 May 2019. It said that MI5 do not know what data is held on "TE 2" nor the associated "working practices" adopted by staff. Mr Jaffey submits that, if those within MI5 responsible for compliance, let alone the IPC or the IPT, do not know the relevant working practices or what data is stored, there cannot have been proper oversight or an effective system of control.

369. Mr Jaffey draws attention to the fact that, in its letter of 26 April 2019, the IPC (enclosing the second inspection report) said:

> "'Annex H' set out that, by 12 April, all business areas would have new processes in place, enabling them to 'account for the handling

> and management of warranted data'. These processes had not all been implemented fully at the time of the inspection. In order to ensure MI5 complies with the IPA's safeguards, their implementation must be completed urgently."

The IPC noted that, despite some progress:

> "Much remains to be done and further, detailed inspections are necessary before I can be assured sufficiently about the lawfulness of MI5's use of [TE] on an ongoing basis."

370. Finally, the Claimant has made submissions about the post-hearing disclosure of the summary and recommendations of Sir Martin Donnelly's Compliance Improvement Review. It submits that, if anything, this shows that MI5's failures have been even worse than had previously thought. For example, the Claimant submits, it has now become apparent that compliance risks were first identified in 2010.

371. Before leaving the documentation we should note what was said in a witness statement filed in these proceedings before this Court on 4 February 2019 by a witness on behalf of MI5, whose identity for understandable reasons has not been disclosed. That witness is a Deputy Director at MI5. The witness manages information and legal compliance teams at MI5 and previously was the MI5 Deputy Legal Advisor. At para. 15 the witness informed the Court that:

> "… I am satisfied that MI5's Handling Arrangements, taken together with the range of internal handling arrangements and policies referred to therein and the information provided in each warrant application, comply with the requirements of the Act. …"

372. Clearly, in the light of the documents that have subsequently been disclosed, that statement has turned out to be wrong, although it is not clear to this Court that it was inaccurate to the knowledge of the witness at the time that it was made. It is to the credit of those acting for the Defendants that they have complied with their duty of candour and co-operation with the Court since that time but it is (to say the least) unfortunate that such disclosure was not made at the time when evidence was filed in these proceedings just a few weeks before the briefing given to the IPC. We do not know the full circumstances and so we say no more about it here.

373. Mr Jaffey submits that not only was there a failure by MI5 to comply with legal requirements as to handling arrangements safeguarding the retention of data obtained pursuant to warrants, there was a breach of the reporting requirement on the part of MI5 since the IPC was not informed of what had gone wrong until February 2019.

374. The provisions of the 2016 Act relating to error reporting by the IPC are contained in section 231. Section 235 enables a JC to carry out such investigations, inspections and audits as he considers appropriate for the purposes of his functions.

375. The Code of Practice on Interceptions of Communications (March 2018) provides, at para. 10.17, that:

> "When a relevant error has occurred, the public authority that made the error must notify the [IPC] as soon as reasonably practicable, and no later than 10 working days after it has been established by appropriate internal governance processes that a relevant error has occurred. Such internal governance processes are subject to review by the [IPC]. Where the full facts of the error cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error."

376. Section 237 provides an "information gateway". It provides that a disclosure of information to the IPC or another JC for the purposes of any function of theirs does not breach either (a) an obligation of confidence owed by the person making the disclosure, or (b) any other restriction on the disclosure of information. This was referred to at the hearing before this Court as a "whistleblowing" provision by Mr Jaffey.

377. Mr Jaffey submits that, despite the fact that the 2016 Act introduced "whistleblowing" provisions to protect someone who might feel the need to make disclosures (in section 237), and despite the fact that lawyers within MI5 were concerned, no-one in fact reported these matters until February 2019. Several years were allowed to elapse since early 2016. Even after the Executive Board of MI5 had considered the matter in October 2018 several more months went by.

378. Mr Jaffey submits that the Defendants have placed great reliance on the existence of effective safeguards, including the *post factum* supervision by the IPC. He reminds this Court that the European Court of Human Rights has frequently said that such supervision by an independent body must be "vested with sufficient powers and competence to exercise an effective and continuous control": see *Zakharov*, at para. 275. He also emphasised, by reference to paras. 284-285 of that judgment, that it is for the respondent Government "to illustrate the practical effectiveness of the supervision arrangements with appropriate examples" and that in *Zakharov* the Court held that supervision by prosecutors of interceptions as it was currently organised was "not capable of providing adequate and effective guarantees against abuse."

379. We are not persuaded in the circumstances of the present case that the same can be said of the legislative scheme of the 2016 Act in this country. The safeguards contained within that Act are capable of preventing abuse. Furthermore, the documents which have been recently disclosed indicate that the IPC is well capable of dealing with the serious issues which have arisen and indeed is dealing with them. He has not considered that MI5 is incapable of putting in place sufficient safeguards in practice for the future.

380. Next Mr Jaffey relied on the decision of the Fifth Section of the European Court of Human Rights in *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (Application No 62540/00, judgment of 30 January 2008), in

particular at paras. 77, 85 and 92. We do not consider that there is an appropriate analogy to be drawn with that case. We note in particular that, at para. 85, the Court said that, unlike the system of secret surveillance which was considered in cases such as *Klass* and *Weber and Saravia*, the Bulgarian legislation did not provide for any review of the implementation of secret surveillance measures by a body or official which was either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring his independence and adherence to the rule of law. No-one outside the services actually deploying special means of surveillance verified such matters as whether those services in fact complied with the warrants authorising the use of such means or whether they faithfully reproduced the original data in the written record. Similarly, there existed no independent review of whether the original data was in fact destroyed within the legal 10-day time limit if the surveillance had proved fruitless. On the contrary, it seemed that all these activities were carried out solely by officers of the Ministry of Internal Affairs. Moreover, it appeared the provisions were applicable only in the context of pending criminal proceedings and did not cover all situations such as the use of special means of surveillance to protect national security. It was for those legal reasons that the Court then turned to consider whether they had an impact on the actual operation of the system in Bulgaria at para. 92 of its judgment. The Court concluded that the system of secret surveillance in Bulgaria was "overused" and that this could in part be due to the inadequate safeguards "which the law provides." It was for that reason the Court concluded, at para. 93, that Bulgarian law did not provide sufficient guarantees against the risk of abuse which is inherent in any system of secret surveillance. It was therefore not in accordance with the law. For that reason there had been a violation of Article 8.

381. Mr Jaffey also placed considerable reliance on two decisions of the IPT. Mr Jaffey readily accepts that the IPT is not one of the courts or tribunals which is able to issue a declaration of incompatibility under the HRA. Nevertheless, he submits, this has not prevented the IPT in practice from assessing the compatibility of legislative schemes with the Convention rights. Further, Mr Jaffey submits, the IPT has engaged in that exercise of assessment not merely by reference to the terms of the legislation alone but also to how it has been applied in practice.

382. The first was *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2016] UKIPTrib 15 110-CH; [2017] 3 All ER 647. In that case the claimant brought proceedings relating to the acquisition, use, retention, disclosure, storage and deletion of bulk personal data sets. The proceedings also concerned the use of section 94 of the Telecommunications Act 1984 by the Secretary of State to give directions to public electronic communications networks to transfer bulk communications data ("BCD") to GCHQ and MI5.

383. The IPT held that, although there was a domestic law power to issue the directions under section 94 of the 1984 Act, this had not sufficiently complied with the Convention concept of law prior to the time when the existence of BPD was publicly avowed by the Respondents in March 2015 and the directions in respect of BCD were publicly avowed in November 2015.

384. In our view, the decision of the IPT in that case is distinguishable for two reasons. First, the IPT was concerned with the requirement that the criteria on which a broadly

worded discretionary power will be exercised should be foreseeable, in other words known to the public.

385. The second reason is that the IPT was not directly concerned with the issue of the compatibility of primary legislation with the Convention rights. It was, as is conventional, concerned with acts of the executive which were alleged to be in breach of the Convention rights and, in particular, on the ground that they were not in accordance with the law. It was in that context that the IPT considered the conduct of the predecessor supervising commissioners to the IPC: see e.g. paras. 79-80 of its judgment. The question which the Court is required to address in the present case is fundamentally different. This Court is being asked to grant a declaration of incompatibility in respect of primary legislation under section 4 of the HRA.

386. Mr Jaffey made similar submissions on the basis of the judgment of the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2018] UKIPTrib 15 110-CH, in particular at paras. 68-71. In that passage the IPT considered the practical steps which the predecessors to the IPC had taken. The IPT was divided, with the majority concluding that the regime in respect of sharing BCD and BPD was compliant with Article 8: see para. 71. The dissenting members of the IPT set out their reasons for dissent in a CLOSED judgment. An application for permission to bring a claim for judicial review has been made to the Administrative Court in respect of that decision of the IPT. In our view that case is distinguishable for the same reasons as above.

387. We should stress that we do not underestimate the seriousness of the matters which have been raised on behalf of the Claimant as a result of the recent disclosure of documents. In our view, however, what they go to is a different question from the one which this Court has to address in these proceedings. That is the question of whether and to what extent MI5 has complied with the requirements of the law either in the past or now. We are also conscious that such matters may be the subject of future litigation, potentially before the IPT (of which one member of this Court, Singh LJ, is the President). Nothing we say in this judgment should be taken to anticipate in any way what might be said in any such future litigation.

388. In the end, we are not persuaded by Mr Jaffey that this issue provides a basis for making a declaration of incompatibility in respect of the 2016 Act. First, the issue is different from the issue of whether acts of the executive may have been unlawful under the Act. The question before this Court now is whether the Act itself is incompatible with the Convention rights.

389. Secondly, and in any event, we are not persuaded that the evidence which has now been made available to the Court in fact proves that the safeguards created by the 2016 Act are insufficient to prevent abuse of the powers under challenge. If anything, as Sir James Eadie submitted to this Court, the fact that this has emerged and the findings which have been made by the IPC in the reports which we have summarised earlier indicate that the system is in truth capable of preventing abuse.

390. Thirdly, we would observe that the recent disclosure has concerned only MI5 and not, for example, the Secret Intelligence Service (MI6) or GCHQ. Yet the Claimant's submission would have the consequence that the 2016 Act as such would be declared to be incompatible with the Convention rights.

391. Finally, it seems to us that Mr Jaffey's submission, if correct, would lead to potentially absurd consequences. Suppose the Claimant were right and there are defects in the 2016 Act which should be the subject of a declaration of incompatibility. Presumably the Claimant would then expect those defects to be remedied by Parliament (or by way of a remedial order). But, however compatible or even "perfect" the Act then was, on the Claimant's case, the fact that MI5 has been found to have defective handling procedures by the IPC would mean that even a new, amended Act could not be implemented. This underlines the point that the defects which have been found do not lead to the necessary consequence that the 2016 Act itself is incompatible with the Convention rights.

392. For those reasons we reject this part of the Claimant's case.

Conclusion

393. The Claimant's Re-amended Statement of Facts and Grounds for Judicial Review in this case was 161 pages long. The Claimant's skeleton argument for the substantive hearing before this Court was 74 pages long. The skeleton argument of the Intervener (the NUJ) was 20 pages long. The Defendants' skeleton argument was 82 pages long. The hearing before us took place over five days. We have taken everything placed before us into account. We trust that we have done justice to the substance of the arguments.

394. We can readily understand that the Claimant, the NUJ and others in society have concerns about the existence of "bulk" powers to obtain large amounts of data, much of which will be of no interest to the intelligence and security agencies. Similar concerns have been expressed both within and outside Parliament. Having had regard to those concerns, Parliament decided to enact the Investigatory Powers Act 2016 in the form which it did. This included a suite of inter-locking safeguards against the possible abuse of power, including the creation of the office of the Investigatory Powers Commissioner.

395. Important though the function of this Court is, the only question which is before us is whether the 2016 Act is compatible with the Convention rights, an exercise which is entrusted to the Court under section 4 of the Human Rights Act 1998.

396. The question which is before this Court has to be addressed against the background that the First Section of the European Court of Human Rights has already held, in the *Big Brother Watch* case, that in principle bulk powers are compatible with the ECHR. There is no requirement for there to be reasonable grounds for suspicion in the case of any individual. For that reason that question was not the subject of argument before this Court but will be considered by the Grand Chamber of the European Court of Human Rights in *Big Brother Watch*.

397. The primary focus of the arguments before this Court has been on the ground that the 2016 Act does not contain sufficient safeguards against the risk of abuse of power and that, accordingly, it is inconsistent with the requirement that interference with human rights must be "in accordance with the law". For the reasons we have given above we do not accept those arguments.

398. Furthermore, we are very conscious that the recent disclosures made by the Defendants about MI5's handling procedures have caused the Investigatory Powers Commissioner obvious concern and will cause others in society concern too. However, for the reasons we have explained above, those matters do not persuade us that the 2016 Act itself is incompatible with the Convention rights. We would also observe that those matters continue to be the subject of further investigation and supervision by the IPC. They may also be the subject of future litigation. It would not be appropriate for this Court to pre-empt anything that might be said in such future proceedings.

399. For the reasons set out in this judgment this claim for a declaration of incompatibility under section 4 of the Human Rights Act 1998 in respect of the Investigatory Powers Act 2016 is refused.

ANNEX:
OVERVIEW OF RELEVANT LEGISLATION

[This document has been agreed between the parties, subject to three "riders" by the Claimant, which are set out below where relevant]

Contents

1. This document presents an overview of the regime introduced by the Investigatory Powers Act 2016 (the "**Act**" or, where clarity requires, the "**2016 Act**"), and certain other relevant legislative provisions. It is intended to be an introduction to the structure and operation of the legislation. It does not refer to all of the relevant provisions for the purposes of the claim.

I) GENERAL PRIVACY PROTECTIONS – PART 1 OF THE ACT

2. The Act sets out "*the extent to which certain investigatory powers may be used to interfere with privacy*": s.1(1).

3. Part 1 of the Act contains both general "*duties in relation to privacy*" and other protections including offences and penalties: s.1(2)-(3).

4. S.2 of the Act contains "general duties" in relation to privacy in s 2(2). The duties apply where a public authority[1] is deciding whether to issue, renew or cancel a warrant under Parts 2, 5, 6 or 7 (as the Secretary of State may do: see below), to approve such a decision (as a Judicial Commissioner may do: see below), to grant, approve or cancel an authorisation under Part 3, or to give a notice under Part 4: s.2(1).

5. In exercising the specified functions, s.2(2) provides that the public authority must have regard to:

> "*(a) whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,*
> *(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation or notice is higher because of the particular sensitivity of that information [2],*
> *(c) the public interest in the integrity and security of telecommunication systems and postal services, and*
> *(d) any other aspects of the public interest in the protection of privacy*".

6. The 'have regard' duties in s.2(2) apply so far as is relevant in the particular context, and subject to the need to have regard to other considerations that are also relevant in that context: s.2(3). Section 2(4) provides that those other considerations may include:

> "*(a) the interests of national security or of the economic well-being of the United Kingdom,*
> *(b) the public interest in preventing or detecting serious crime,*
> *(c) other considerations which are relevant to –*
> *(i) whether the conduct authorised or required by the warrant, authorisation or notice is proportionate, or*
> *(ii) whether it is necessary to act for a purpose provided for by this Act,*
> *(d) the requirements of the Human Rights Act 1998, and*
> *(e) other requirements of public law.*"

7. Part 1 of the Act also contains certain criminal offences, namely, intentional "unlawful interception" (s.3) and knowingly or recklessly "unlawfully obtaining communications data" (s.11).

8. *Unlawful interception* occurs where (a) a person intentionally intercepts[3] a communication in the course of its transmission by a public or private telecommunications system or a public postal service, (b) the interception is carried out in the UK and (c) the person lacks "*lawful authority*" to do so: s.3(1). So far as is material to the present claim, lawful authority will exist (inter alia) where the interception is carried out in accordance with a bulk interception warrant under Pt 6,

---

[1] Defined as "*a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal*": s.263(1).

[2] Section 2(5) gives certain examples of sensitive information for these purposes, including "*items subject to legal privilege*" and "*any information identifying or confirming a source of journalistic information*".

[3] Interception (etc.) for these purposes is defined in s.4 of the Act. In summary, it consists of doing a 'relevant act' in relation to a system (namely modifying or interfering with the system or its operation, monitoring transmissions made by means of the system, or monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system), whose effect is to make the content of any communication available to a person who is not the sender or intended recipient of the communication.

Ch 1 of the Act: s.6(1)(a)(ii). The offence of unlawful interception is triable 'either way', and, on conviction on indictment, a person guilty of it is liable to up to 2 years' imprisonment or a fine (or both): s.3(6). Section 7 of the Act makes provision for the imposition of monetary penalties (of up to £50,000) by the Investigatory Powers Commissioner in cases of interception without lawful authority which do not, in the Commissioner's view, amount to the offence of unlawful interception, but this provision does not apply where a person was "*making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception*".

9. *Unlawfully obtaining communications data* occurs where, without lawful authority[4], a relevant person[5] knowingly or recklessly obtains communications data from a telecommunications operator or postal operator: s.11(1). It is a defence if the person can show that s/he acted in the reasonable belief that s/he had lawful authority to obtain the communications data. The offence of unlawfully obtaining communications data is also triable 'either way', and, on conviction on indictment, a person guilty of it is liable to up to 2 years' imprisonment or a fine (or both): s.11(4)(d).

II) BULK INTERCEPTION, ACQUISITION AND EQUIPMENT INTERFERNCE WARRANTS – PART 6

10. This claim concerns, inter alia, the 'bulk warrant' provisions in Part 6. In that regard:

    a. Pt 6 Ch 1 provides for bulk interception warrants.

    b. Pt 6 Ch 2 provides for bulk acquisition warrants (for communications data).

    c. Pt 6 Ch 3 provides for bulk equipment interference warrants.

11. The key provisions are set out below (bulk personal datasets, under Pt 7 of the Act, are considered separately).

(a) Bulk interception warrants (Pt 6 Ch 1)

12. A bulk interception must satisfy the following two cumulative conditions:

    a. Its "*main purpose*" is either the interception of "*overseas-related*" communications (i.e. communications sent or received by individuals who are outside the British Islands) or the obtaining of "*secondary data*" from such communications (s.136(2)); and

    b. The warrant authorises or requires its addressee to secure, by any conduct described in the warrant, one or more of (a) the interception, in the course of

[4] S.81 makes provision for the circumstances in which conduct authorised by Pt 3 ('*Authorisations for obtaining communications data*') will be considered to be lawful.
[5] Defined in s.11(2) as a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).

their transmission by means of a telecommunication system, of "*communications*" described in the warrant; (b) the obtaining of "*secondary data*" from such communications; (c) the "*selection for examination*", in any manner described in the warrant, of "*intercepted content*" or "*secondary data*" obtained under the warrant; or (d) the "*disclosure*", in any manner described in the warrant, of anything obtained under the warrant to its addressee or any person acting on their behalf (s.136(4)).

13. A bulk interception warrant also authorises any conduct which it is necessary to undertake in order to do what is expressly authorised or required (s.136(5)).

14. "*Communication*" by s 261(1) relevantly includes "*anything comprising speech, music, sounds, visual images of data of any description*" and "*signals serving either for the impartation of anything*" between persons or things (or both) "*or for the actuation or control of any apparatus*". A communication may therefore be or contain "*content*" and/or "*secondary data*" (see immediately below).

15. "*Content*" by s 261(6) means relevantly "*any element of* [a] *communication, or any data attached to or logically associated with* [a] *communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but — (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and (b) anything which is systems data is not content.*" (By s 157(1), "*intercepted content*" in relation to a bulk interception warrant means "*any content of communications intercepted by an interception authorised or required by the warrant*".)

16. "*Secondary data*" by s 137 means either of the following:

    a. First, "*systems data*" which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise) (s 137(4)). "*Systems data*" means "*any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of*" a postal service, a telecommunications system (including any apparatus that forms part of it), any telecommunications service provided by means of a telecommunication system, any system on which communications or other information are held (including any apparatus forming part of it) (a "*relevant system*"), and any service provided by means of a relevant system (s.263(4)–(5)).

    b. Secondly, "*identifying data*" that—(a) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise), (b) is capable of being logically separated from the remainder of the communication, and (c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication (s.137(5)). "*Identifying data*" means data which may be used to identify, or assist in identifying, any person, apparatus, system, service, event or the location of any person, event or thing (s.263(2)–(3)).

(b) Bulk acquisition warrants (Pt 6 Ch 2)

17. Bulk acquisition warrants authorise the obtaining, imposition of a requirement to obtain, "*selection for examination*" and disclosure of "*communications data*".

18. Specifically, a bulk acquisition warrant authorises or requires its addressee to secure, by any conduct described in the warrant, any one or more of (see s.158(5) and (6)):

    a. requiring a telecommunications operator specified in the warrant (i) to disclose to a person specified in the warrant any "*communications data*" which is specified in the warrant and is in the possession of the operator, (ii) to obtain any communications data specified in the warrant which is not in the operator's possession but which the operator is capable of obtaining, or (iii) to disclose to a person specified in the warrant any data so obtained;

    b. the selection for examination, in any manner described in the warrant, of communications data obtained under the warrant;

    c. the disclosure, in any manner described in the warrant, of communications data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

19. "*Communications data*" ("**CD**") is defined in s.261(5), as follows:

> "'*Communications data*', *in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data –*
> *(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and –*
> *(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,*
> *(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or*
> *(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,*
> *(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or*
> *(c) which –*
> *(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,*
> *(ii) is about the architecture of a telecommunication system, and*
> *(iii) is not about a specific person,*
> *but does not include any content of a communication or anything which, in the absence of subsection (6)(b), would be content of a communication.*"

20. Bulk acquisition warrants again authorise any conduct necessary to undertake what is expressly authorised or required and any conduct by a person required to assist giving effect to the warrant (s.158(7)).

(c) Bulk equipment interference warrants (Pt 6 Ch 3)

21. A bulk equipment interference warrant (s.176(1)):

    a. authorises or requires its addressee to "*secure interference with any equipment*" for the purpose of obtaining "*communication*", "*equipment data*" or "*any other information*"; and

    b. has as its "*main purpose*" to obtain "*overseas-related*" communications, information or equipment data.

22. In Pt 6 Ch 3:

    a. "*Communication*" again includes (a) anything comprising speech, music, sounds, visual images or data of any description and (b) signals serving either for the impartation of anything between persons or things (or both) or for the actuation or control of any apparatus (s.198(1)).

    b. "*Equipment*" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment (s.198(1)).

    c. "*Equipment data*" means either:

        i. "*Systems data*" (as defined in paragraph 16 above); or

        ii. "*Identifying data*" (as defined in paragraph 16 above) that is comprised in, part of, attached to or logically associated with, and is capable of being logically separated from, a communication or any other item of information without revealing anything of what might reasonably be considered to be the meaning of that communication / item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact (s.177(1)(b), (2)).

    d. "*Overseas-related information*" means information of individuals who are outside the British Islands (s.176(2)).

    e. "*Overseas-related communications*" are communications sent or received by individuals outside the British Islands (s.176(2)).

    f. "*Overseas-related equipment data*" means "*equipment data*" which (a) forms part of, or is connected with, overseas-related communications or overseas-related information, (b) would or may assist in establishing the existence of overseas-related communications or overseas-related information or in obtaining such communications or information, or (c) it would or may assist in developing capabilities in relation to obtaining overseas-related communications or overseas-related information (s.176(3)).

23. A bulk equipment interference warrant (s.176(4)):

    a. must authorise or require the person to whom it is addressed to secure the obtaining of the communications, equipment data or other information to which the warrant relates; and

    b. may also authorise or require the person to whom it is addressed to secure:

        i. the selection for examination, in any manner described in the warrant, of any material so obtained; and/or

        ii. the disclosure, in any manner described in the warrant, of any such material to the addressee or any person acting on their behalf.

24. Again, bulk equipment interference warrants authorise any conduct necessary to undertake what is expressly authorised or required and any conduct by a person required to assist giving effect to the warrant: s.176(5).

(d) Criteria for approval of bulk intercept, acquisition and equipment interference warrants by the Secretary of State

25. In the case of all three types of bulk warrant in Part 6, the power to issue a warrant resides with the Secretary of State, and is exercisable only following an application made by or on behalf of the head of an intelligence service (s.138(1), s.158(1) and s.178(1)).

26. In each case, the Secretary of State may only issue the warrant if s/he considers that:

    a. the warrant is necessary in the interests of national security[6] or on that ground and for the purpose of preventing or detecting serious crime and/or in the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security[7]; and

    b. the conduct authorised by the warrant is proportionate[8] to what is sought to be achieved by that conduct[9];

    c. each of the specified "*operational purposes*" (see below) is a purpose for which the examination of material obtained under the warrant is or may be necessary, and the examination of material for each such purpose is necessary

[6] s.138(1)(b)(i), s.158(1)(a)(i), s.178(1)(b)(i).

[7] s.138(1)(b)(ii) and (2), s.158(1)(a)(ii) and (2), s.178(1)(b)(ii) and (2). A warrant may be considered necessary on the "economic well-being" ground only if the information / communications data which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands (s.138(3), s.158(3)) or if the interference with equipment which would be authorised by the warrant is considered necessary for the purposes of obtaining information relating to the acts or intentions of persons outside the British Island (s178(3)).

[8] The requirements of necessity and proportionality are addressed in Interception CoP, §§6.22-6.26; Bulk Acquisition CoP, §§4.6-4.11; Bulk EI CoP, §§6.15-6.19.

[9] s.138(1)(c), s.158(1)(b), s.178(1)(c).

on any of the grounds on which the Secretary of State considers the warrant to be necessary[10];

d. satisfactory arrangements made for the purposes of safeguards relating to disclosure etc. (see below) are in force in relation to the warrant[11];

e. the decision to issue the warrant has been approved by a Judicial Commissioner[12]. However, in relation to bulk equipment interference only, the requirement for prospective Judicial Commissioner approval does not apply where the Secretary of State considers that there is an urgent need to issue the warrant (see below for the provisions that require retrospective Judicial Commissioner approval in such cases).

27. In the case of bulk interception warrants and bulk equipment interference warrants only, the Secretary of State must additionally consider that:

a. in the case of bulk interception warrants, the main purpose of the warrant is the interception of overseas-related communications and/or the obtaining of secondary data from such communications (s138(1)(a)); and

b. in the case of bulk equipment interference warrants, the main purpose of the warrant is to obtain overseas-related communications, overseas-related information or overseas-related equipment data (s.178(1)(a)).

28. Detailed provision as to the format of, and the matters that must be included in, warrant applications under Part 6 Chs 1-3 of the Act appears at: §§6.17-6.20 of the Interception of Communications Code of Practice (the "**Interception CoP**") (bulk interception warrants); §§4.1-4.5 of the Bulk Acquisition of Communications Data Code of Practice (the "**Bulk Acquisition CoP**") (bulk acquisition warrants); and §§6.10-6.13 of the Equipment Interference CoP (the "**EI CoP**") (bulk equipment interference warrants).

29. In relation to all three types of bulk warrant, the decision to issue a warrant must be taken personally by the Secretary of State, and the warrant must be signed by the Secretary of State (s.141, s.160, s.182)[13].

30. Each of the three forms of bulk warrant under Pt 6 Chs 1-3 must, as issued, contain a provision stating that it is a bulk warrant of that kind and it must be addressed to the head of the intelligence service by whom or on whose behalf the warrant application was made; and it must describe the conduct that is authorised by the warrant (s.142(1)-(2), s.161(1)-(2), s.183(1)-(2)[14]). It must also specify the operational purposes for which any material obtained under the warrant may be selected for examination: see under "Operational Purposes" below.

---

[10] s.138(1)(d), s.158(1)(c), s.178(1)(d)
[11] s.138(1)(e), s.158(1)(d), s.178(1)(e)
[12] s.138(1)(g), s.158(1)(e), s.178(1)(f).
[13] Bulk equipment interference warrants may be signed by a designated senior official if it is not reasonably practicable for the warrant to be signed by the Secretary of State: ss.182(3)–(4) and EI CoP §§6.21-6.22.
[14] In the case of a bulk equipment interference warrant, the warrant must also "*describe the conduct that is authorised by the warrant*" (s.183(3)).

(e) **Necessity and proportionality**

31. Warrants under Pts 6 Ch 1-3 of the Act may only be issued where the Secretary of State considers a warrant to be necessary for the specified statutory purposes (i.e. national security, or national security *together with* the prevention / detection of serious crime or the interests of the economic well-being of the UK (so far as also relevant to the interests of national security), and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct, including whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means (see s.2(2)(a) of the Act, as referred to above).

(f) **Operational purposes**

32. The Secretary of State may not issue a bulk warrant under Pt 6 Ch 1, 2 or 3 unless s/he considers that (i) each of the "*specified operational purposes*" is a purpose for which the examination of material obtained under the warrant is or may be necessary, and (ii) the examination of material for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary: s.138(1)(d), s.158(1)(c), s.178(1)(d).

33. In that regard, a bulk warrant under each of Pt 6 Chs 1-3 must "*specify the operational purposes for which any [material] obtained under the warrant may be selected for examination*" (s.142(3), s.161(3), s.183(4)).

34. By ss.142(4)-(11), 161(4)-(11) and 183(5)-(12):

    a. The operational purposes specified in a warrant must be in a "*list of operational purposes*" maintained by the heads of the intelligence services as purposes which they consider are operational purposes for which material obtained under the type of bulk warrant may be selected for examination.

    b. An operational purpose may be specified in that list only with the approval of the Secretary of State, who may give such approval only if satisfied that the operational purpose is "*specified in a greater level of detail than*" "*national security*", "*preventing or detecting serious crime*" or "*the economic well-being of the United Kingdom so far as … relevant to the interest of national security*".

    c. The list of operational purposes must be provided by the Secretary of State to the Intelligence and Security Committee of Parliament every three months. The Prime Minister must review the list of operational purposes at least once a year.

    d. A warrant may specify all of the operational purposes which, at the time the warrant is issued, are specified in the list of operational purposes.

    e. The Codes of Practice indicate that the practice will (other than in exceptional circumstances) always be that *all* operational purposes (for the type of warrant) are included in every warrant: Interception CoP §6.67-6.68; Bulk Acquisition CoP §6.10; EI CoP §§6.6-6.7.

35. Interception CoP §§6.61-6.67 makes further provision relating to operational purposes.[15]

(g) **Existence of safeguards**

36. Warrants in respect of the bulk powers in Pt 6 Chs 1–3 may only be issued if the Secretary of State considers that satisfactory "*safeguards*" are in place in respect of a number of matters: s.138(1)(e), s.158(1)(d), s.178(1)(e). Again, the relevant safeguards are largely the same in relation to each of the three key bulk powers.

(i) Safeguards relating to retention, copying and disclosure

37. In relation to every bulk (Pt 6) warrant, the Secretary of State must ensure that arrangements are in force for securing that:

    a. In relation to material obtained under the warrant, each of the following is limited to the minimum that is necessary for the "*authorised purposes*":

        i. the number of persons to whom any of the material is disclosed or otherwise made available;

        ii. the extent to which any of the material is disclosed or otherwise made available;

        iii. the extent to which any of the material is copied; and

        iv. the number of copies that are made;[16]

    and

    b. every "*copy*" made of any "*material*" obtained under a warrant is destroyed as soon as there are no longer any "*relevant grounds*" for retaining it[17];

    and

    c. specific safeguards relating to the examination of material are also in place[18] (see "Safeguards relating to selection for examination" below).

38. As to (a), the meaning of "*necessary for the authorised purposes*" is elucidated in the same terms for each of the three bulk powers: see s.150(3), s.171(3) and s.191(3)[19]. The

[15] And see Bulk Acquisition CoP §6.3 *et seq*, EI CoP §6.67 *et seq*.

[16] See s.150(1)(a) and (2); s.171(1)(a) and (2); and s.191(1)(a) and (2).

[17] See s.150(1)(a) and (5); s.171(1)(a) and (5); and s.191(1)(a) and (5). There will no longer be any relevant grounds for retaining a copy of any material if, and only if, "*(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or [national security together with one of the other specified grounds], and (b) its retention is not necessary for any of the purposes mentioned [in s.150(3)(b)-(e), s.171(3)(b)-(e) or s.191(3)(b)-(e) as the case may be]*": see s.150(1)(6), s.171(1)(6), s.191(1)(6). "Copy" has a statutory definition: see s.53(10) in relation to interception, s.191(9) in relation to material obtained under a bulk EI warrant, s.171(10) in relation to material obtained under a Bulk Acquisition warrant.

[18] See s.150(1)(b); s.171(1)(b); and s.191(1)(b)

[19] Specifically, "*something is necessary for the authorised purposes if, and only if –*

#

arrangements for ensuring that the requirements in s.150(2), s.171(2) and s.191(2) are met (i.e. that the various specified matters are kept to the minimum necessary for the authorised purpose) must include "*arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner*": s.150(4), s.171(4) and s.191(4).

39. However, where material obtained under a warrant (or a copy) has been provided to any overseas authority, these safeguards do not apply: s.150(8), s.171(8) and s.191(8). Instead, the Secretary of State must ensure that requirements corresponding to those immediately above and immediately below apply "*to such extent (if any) as the Secretary of State considers appropriate*": see s.151(1) and (2)(a), s.171(9) and s.192(1)-(2).[20]

40. Pt 6 Ch 1 and Pt 6 Ch 3 contain statutory duties not to make "*unauthorised disclosures*" (s.156 and s.197), including disclosure of any material obtained under bulk interception or bulk equipment interference warrants, save where the disclosure is an "*excepted disclosure*" (including a disclosure authorised by the warrant, a disclosure to oversight bodies, etc.). It is a criminal offence to make an "*unauthorised disclosure*" of this kind[21]. Under Pt 6 Ch 2, s.174 makes it an offence for the telecommunications operator required to assist with the warrant (or a person employed or engaged for its business) to disclose the existence or contents of the warrant itself, but there is no offence of disclosing what is collected under a bulk acquisition warrant.

41. Each relevant CoP contains provisions addressing retention, copying and disclosure: Interception CoP §§9.15-9.31; Bulk Acquisition CoP §§9.4-9.13; EI CoP §§9.1-9.35.

(ii) Safeguards relating to selection for examination

42. The Act also requires the Secretary of State to ensure that safeguards relating to the examination of material are in force before issuing a bulk interception warrant, a bulk acquisition warrant or a bulk equipment interference warrant (ss.150(1)(b) and 152; ss.171(1)(b) and 172; and ss.191(1)(b) and 193)). Specifically, s/he must ensure that:

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 138(2),
(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is or was addressed,
(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,
(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or
(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923."

[20] In the case of bulk interception warrants, the Secretary of State must additionally ensure that restrictions are in force which would "*prevent, to such extent (if any) as the Secretary of State considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in a prohibited disclosure*": s.151(1) and (2)(b). Under s.151(3), "*prohibited disclosure*" means a disclosure which, if made in the United Kingdom, would breach the prohibition in s.56(1) of the Act, which provides that no evidence may be adduced (etc.) in legal proceedings which either discloses, in circumstances from which its origin in 'interception-related' conduct may be inferred, any content of an interception communication or any secondary data obtained therefrom, or which tends to suggest that any interception-related conduct has or may have occurred or is going to occur. (Interception-related conduct is defined in s.56(2) and, read with s.156(1), covers matters such as the making of an application by any person for a warrant, or the issue of warrant, under Pt 6 Ch 1.) The prohibition in s.56(1) is subject to various exceptions set out in Schedule 3.

[21] See: ss.57-59 and 156 (bulk interception warrants); ss.132-134 and 197 (bulk interception warrants).

a. The "*selection for examination*" of any material obtained under a warrant is carried out only in so far as is "*necessary for the operational purposes specified in the warrant*" at the time of the selection for examination (ss.152(1)(a), (2), 172(1)(a), (2)-(3) and 193(1)(a), (2)); and

b. The selection of any of such material is "*necessary and proportionate in all the circumstances*" (ss.152(1)(b), 172(1)(b), 193(1)(b)).

43. Because an operational purpose may be included in a warrant for any of the purposes for which a warrant is issued, "*selection for examination*" may occur for "*operational purposes*" considered necessary for any of "*national security*", "*preventing or detecting serious crime*" or "*the economic well-being of the United Kingdom*" insofar as relevant to national security.

44. In relation to bulk interception warrants and bulk equipment interference warrants, the Secretary of State must also ensure that the selection for examination of respectively "*content*" and "*protected material*" meets any of the "*selection conditions*" (s.152(1)(c) and s.193(1)(c)) (the "**British Islands safeguard**".) The selection conditions are as follows (s.152(3) and s.193(3)):

a. Selection of the material for examination does not breach the prohibition on the use of selection criteria that are (i) referable to an individual known to be in the British Islands at that time and (ii) used for the purpose of identifying (a) the content of communications sent by or intended for that individual (for a bulk interception warrant) or (b) "*protected material*"[22] consisting of communications sent by, or intended for, that individual or "*private information*" relating to that individual (for bulk equipment interference warrants): ss.152(3)(a) and (4), 193(3)(a) and (4). Sections 152(4) and 193(4) respectively prohibit such selection for examination.

b. The warrant addressee "*considers*" (for a bulk interception warrant) or "*reasonably considers*" (for a bulk equipment interference warrant) that the selection for examination does breach that prohibition: ss.152(3)(b) and 193(3)(b));

c. The selection for examination of the "*content*" / "*protected material*" in breach of the prohibition is authorised by, respectively, s.152(5) or s.193(5), which authorise selection for examination where someone enters the British Islands or it becomes apparent that a belief that they were not in the British Islands was mistaken and a "*senior officer*" authorises continued selection for examination for up to five working days[23]; or

[22] Meaning any material obtained under the warrant other than material which is equipment data (see definition at §22.c above) or information (other than a communication or equipment data) which is not private information: s.193(9).

[23] These dis-apply the prohibition on selection for examination of material referable to a person known to be in the British Islands for the purpose of identifying their communications or where (a) criteria referable to an individual have been, or are being, used for the selection for examination of "*content*" / "*protected material*" in circumstances where the prohibition was not breached (or the addressee of the warrant considers it would not be breached, in the case of a bulk interception warrant, or reasonably considers it would not be breached, in the case

#

d. Selection for examination of the "*content*" / "*protected material*" in breach of the prohibition is authorised by a targeted examination warrant issued under either Ch 1 Pt 2 or Pt 5.

Claimant's "rider":

(1) The British Islands safeguard in s 193(1)(c) for bulk interception warrants and bulk equipment interference warrants applies only to "*selection for examination*" of "*content*" (s 152(1)(c)) and "*protected material*" (s 193(1)(c)) respectively and not to other material obtained under a warrant. This is a central feature of this safeguard.

(2) There is no British Islands safeguard for bulk acquisition warrants under Pt 6 Ch 2.

45. The relevant Codes of Practice make further provision in relation to selection for examination: Interception CoP §6.71 *et seq*, Bulk Acquisition CoP §6.14 *et seq*; EI CoP §6.66 *et seq*.

(iii) Enhanced safeguards – special cases

Legally privileged material: bulk interception and bulk EI

46. **Basic position:** As to legally privileged material, the basic position for bulk interception and bulk equipment interference warrants is that:

a. Where "*intercepted content*" / "*protected information*" is selected for examination using criteria the (or a) purpose of which is, or use of which is likely, to identify legally privileged items, a senior official acting on behalf of the Secretary of State must approve the use of such criteria, having regard to "*the public interest in the confidentiality of the items subject to legal privilege*": ss.153(1)-(2), 194(1)-(2).

b. Approval may be given only if the official considers that there are specific arrangements in place for the handling, retention, use and destruction of items subject to legal privilege: ss. 153(4)(a), 194(4)(a).

c. In addition, where the (or a) purpose of using the criteria is to identify legally privileged items (but not otherwise, in particular not where the use of such criteria is likely to identify privileged items), approval may be given only if there are "*exceptional and compelling circumstances that make it necessary to*

---

of a bulk equipment interference warrant), (b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual which would mean that the selection of the relevant content for examination would breach the prohibition, (c) since that time, a written authorisation to examine the relevant content using those criteria has been given by a senior officer, and (d) the selection of the relevant content for examination is made before the end of the "permitted period", being the fifth working day after the time at which the relevant change in circumstances appears to the addressee of the warrant: ss.152(5)(d) and (7); 193(5)(d) and (7)). "*Relevant change of circumstances*" means either that the individual concerned has entered the British Islands or that the addressee of the warrant was mistaken in believing that the individual was outside the British Islands: ss.152(6), 193(6).

authorise the use of the relevant criteria": ss.153(4), 194(4). An exhaustive definition of exceptional and compelling circumstances is set out in the Act (ss.153(5) and 194(5)).

47. **Communications furthering a criminal purpose:** Where the (or a) purpose of the use of criteria for selection for examination of "*intercepted content*" / "*protected information*" (but not other material obtained under a warrant) is to identify communications / information that would be subject to legal privilege if they were not made / created or held with the intention of furthering a criminal purpose, one of the "selection conditions" is met (see above) and the warrant addressee considers that the items are "*likely to be communications made with the intention of furthering a criminal purpose*", the selection for examination may occur only if a "*senior official*" has approved the criteria: ss.153(6)-(7), 194(6)-(7). Approval may be given only if the official "*considers*" that the items "*are likely to be*" made / held or created "*with the intention of furthering a criminal purpose*": ss.153(8), 194(8).

48. **Where targeted examination warrants are required and the purpose is to select privileged items:** Where a targeted examination warrant is required in order to select for examination items subject to legal privilege[24] and the (or a) purpose is to authorise the selection for examination of items subject to legal privilege, s.27 and s.112 provide that: the warrant application must state that purpose; the person determining the application must have regard to the public interest in the confidentiality of items subject to legal privilege; and the person determining the application must issue a warrant only if s/he considers that (i) there are exceptional and compelling circumstances that make it necessary to select such items for examination and (ii) the relevant safeguards include specific arrangements for the handling, use, retention and destruction of such data (s.27(2)-(4), s.112(2)-(4)). The same definition of exceptional and compelling circumstances is used in s.27(6) and s.112(6).

49. **Retention following selection for examination:** Where an item subject to legal privilege is retained following its examination for a purpose other than its destruction, the addressee of the warrant must inform the Investigatory Powers Commissioner ("**IPC**") as soon as is reasonably practicable. The IPC must, unless he considers that the public interest in retaining the item outweighs the public interest in its confidentiality, and that retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury, direct that the item is destroyed or impose conditions as to the use/retention of the item: ss.153(9)-(12), 194(9)-(12).

Claimant's "rider":

The provisions in Pt 6 Ch 1 and Pt 6 Ch 3 that empower the IPC to give directions in relation to legally privileged material (ss 153(9)–(12) and 194(9)–(12)) do not prohibit the use of dissemination of the material before the IPC makes a determination. No equivalent provisions exist in Pt 6 Ch 2.

[24] i.e. where the British Islands safeguard applies (and other "selection criteria" do not authorise selection for examination): see s.152(3)(d) (bulk interception), s.193(3)(d) (bulk equipment interference).

50. **Definition of "legal privilege":** "Items subject to legal privilege", in relation to England and Wales, has the same meaning as in s.10 Police and Criminal Evidence Act 1984; other definitions apply to Scotland and Northern Ireland: see s.263.

51. **CoP provision:** The safeguards applicable to the selection for examination of legally privileged material are explained at §9.48 *et seq* of the Interception CoP and §9.55 of the EI CoP. Among other matters, pursuant to the Interception CoP and Bulk EI CoP:

    a. Where an application for a targeted examination warrant is made where the (or a) purpose is to obtain items that would be subject to legal privilege, if they were not made with the intention of furthering a criminal purpose, the application must contain a statement to that effect and the reasons for believing that the criminal purpose exception applies: Interception CoP §9.57; Bulk EI CoP §9.53.

    b. Wherever a person to whom a targeted examination warrant relates is a lawyer known to be acting in a professional capacity, or where communications are to be selected for examination using criteria referable to such a person, the authority must assume that the statutory protections for legally privileged material apply: Interception CoP §9.62; Bulk EI CoP §9.58.

    c. In the event that privileged communications are inadvertently and unexpectedly selected for examination (so that the enhanced procedure has not been followed), any content so obtained must be handled strictly in accordance with ss.153/194, and the applicable provisions of the Codes, and no further privileged material may be intentionally selected for examination by reference to those criteria unless approved by a senior official: Interception CoP §9.61; EI CoP §9.57.

    d. An authority will not act on or further disseminate legally privileged items without first informing the IPC that the items have been obtained or selected for examination, save where there is an urgent need to take action and it is not reasonably practicable to inform the IPC. In such cases, the agency should wherever possible consult a legal adviser. See Interception CoP §9.71; EI CoP §9.67.

<u>Journalists: bulk interception and bulk EI</u>

52. Relevant statutory safeguards apply to (i) "confidential journalistic material" (as defined in s.264[25]); and (ii) "sources of journalistic information" (as defined in s.263).

53. In relation to confidential journalistic material, where such material is retained following its examination for a purpose other than its destruction, the addressee of the warrant must inform the IPC as soon as is reasonably practicable: ss.154, 195.

Claimant's "rider":

The provisions in Pt 6 Ch 1 and Pt 6 Ch 3 that require reporting to the IPC where "*confidential journalistic material*" is retained (ss 154 and 195) do not prohibit the use of

[25] S.264 contains statutory definitions of "*journalistic material*" and "*confidential journalistic material*".

dissemination of the material before the IPC makes a determination. No equivalent provisions exist in Pt 6 Ch 2.

54. Additional statutory safeguards apply where a targeted examination warrant is required[26] and the (or a) purpose is the selection for examination of "*journalistic material*" which the authority believes is "*confidential journalistic material*". The warrant application must contain a statement that the purpose is to select such material for examination; and the person to whom the application is made may issue the warrant only if they consider that the arrangements under s.150 or s.191 (as the case may be) include specific arrangements for the handling, retention, use and destruction of communications containing confidential journalistic material: see s.28(2), s.113.

55. The same applies, *mutatis mutandis,* where an application is made for a targeted examination warrant for the (or a) purpose of identifying a source of journalistic information i.e. the application must so state; and the person issuing the warrant must consider that appropriate arrangements are in place: s.29, s.114.

56. Under the Codes:

    a. Where an authorised person intends to select content or secondary data for examination in order to identify or confirm a source of journalistic information (and where it is not necessary to apply for a targeted examination warrant) s/he must notify a senior official[27] before so doing, and may not select the material for examination unless s/he has received the official's approval. The senior official may not provide such approval unless s/he considers that the agency has arrangements in place for the handling, retention, use and destruction of communications that identify sources of journalistic information. The same applies to the selection for examination of content in order to obtain confidential journalistic material. See Interception CoP §§9.84-9.86; Bulk EI CoP §§9.84-9.86.

    b. Where confidential journalistic material, or material identifying a journalistic source, is retained and disseminated to an outside body, reasonable steps should be taken to mark the disseminated information as confidential: Interception CoP §9.87; Bulk EI CoP, §9.80.

    c. The EI Code provides that where an application is made for a targeted examination warrant to identify a source, the *"public interest requiring such selection must override any other public interest"*: EI Code, §9.76.

<u>Bulk Acquisition: lawyers and journalists</u>

57. The Bulk Acquisition CoP contains specific protections for the selection of data for examination in such cases:

    a. The Bulk Acquisition CoP requires officers to take into account any circumstances that might lead to an unusual degree of intrusion when selecting

[26] i.e. where the British Islands safeguard applies (and none of the other "*selection conditions*" is met).
[27] As defined in s.145.

data for examination. Such circumstances are specifically stated to include *"all cases where it is intended or known that the data being selected for examination includes communications data of…lawyers, journalists…"*: §6.23.

b. Further provision is made as to journalists:

i. The selection for examination of data in order to determine a source of journalistic information requires prior approval from a person holding the rank of Director or above, and any communications data so obtained and retained must be notified to the IPC at the next inspection: §6.28. This does not apply where the intent is to examine a journalist's communications data but not intended to determine the source of journalistic information: §6.30.

ii. Further, where a journalist's data is selected, but the intention is not to determine a source of journalistic information, particular care must be taken to ensure that the officer considers whether the intrusion is justified, giving proper consideration to the public interest, and whether there are alternative means for obtaining the information: §6.31.

(iv) Offences

58. The Act creates specific criminal offences that apply where a person deliberately selects material for examination that breaches the examination safeguards referred to above, knowing or believing that doing so will breach the safeguard: see ss.155, 173, 196. Such an offence is punishable on conviction on indictment by imprisonment for up to 2 years or an unlimited fine.

(h) **Requirement for independent approval of warrants by a Judicial Commissioner**

(i) General position (non-urgent warrants)

59. In the case of all three types of bulk warrant in Part 6, the Secretary of State's power to issue a warrant is subject to a requirement to obtain independent approval by a Judicial Commissioner (ss.140, 159, 179). The Judicial Commissioner is required to review the Secretary of State's conclusions as to:

a. whether the warrant is necessary, by reference to the purpose for which the warrant is sought (e.g. national security);

b. whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;

c. Whether each of the specified operational purposes is a purpose for which the examination of the content/data obtained is or may be necessary;

d. Whether the examination of content/data for each purpose is necessary on any of the grounds on which the Secretary of State considered the warrant to be necessary.

60. The Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review and must consider matters with a sufficient degree of care as to ensure that s/he complies with the general duties in relation to privacy imposed by s.2.

61. Where a Judicial Commissioner refuses to approve a decision to issue a warrant, s/he must give written reasons to the Secretary of State, and the Secretary of State may in that case ask the IPC (unless he was the Judicial Commissioner who gave the refusal) to decide whether to approve the decision to issue the warrant.

(ii) Judicial Commissioner approval of bulk equipment interference warrants in urgent cases

62. As set out above, in relation to bulk equipment interference warrants only, the Secretary of State is not required to obtain advance approval from a Judicial Commissioner in urgent cases: s.178(1)(f).

63. In such a case, the Secretary of State must inform a Judicial Commissioner that a warrant has been issued, following which that Judicial Commissioner must (before the end of the third working day after the day on which the warrant was issued) decide whether to approve the decision to issue the warrant, and notify the Secretary of State of that decision. If the Judicial Commissioner refuses to approve the decision, the warrant ceases to have effect (unless already cancelled) and may not be renewed: s.180. Where this occurs, the person to whom the warrant was addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible: s.181(2). The Judicial Commissioner may (a) authorise further interference with equipment for the purpose of enabling the person to secure that anything in the process of being done under the warrant stops as soon as possible, (b) direct that any material obtained under the warrant is destroyed; and/or (c) impose conditions as to the use or retention of any of that material: s.181(3). In exercising these functions, the Judicial Commissioner may require an 'affected party' (being both the Secretary of State and the addressee of the warrant) to make representations, and must have regard to any representations made by an affected party (whether or not such representations were required): ss.181(4)-(5).

64. The Secretary of State may ask the IPC to review a decision made by any other Judicial Commissioner under s.181(3), whereupon the IPC may confirm the decision or make a fresh one: s.181(7).

65. Nothing in ss.180 or 181 affects the lawfulness of anything done under a warrant before it ceases to have effect, or anything being done under a warrant when it ceases to have affect before that thing could be stopped or that it is not reasonably practicable to stop: s.181(8).

(i) **Duration, modification and cancellation of bulk warrants**

66. As to duration, bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants (unless already cancelled) cease to have effect at the end of the period of 6 months beginning with (a) the day on which the warrant was issued, or (b) in the case of a warrant that has been renewed, the day after the day at

the end of which the warrant would have ceased to have effect if it had not been renewed: ss.143, 162, 184(1) and (2)(b)[28].

67. As to renewal, the Secretary of State may renew a bulk interception warrant, bulk acquisition warrant or a bulk equipment interference warrant at any time during the period of 30 days ending with the day at the end of which the warrant concerned would otherwise cease to have effect, provided that certain "*renewal conditions*" are met. The relevant renewal conditions in each case are as follows:

> "*(a) that the Secretary of State considers that the warrant continues to be necessary –*
>
> *(i) in the interests of national security, or*
>
> *(ii) on that ground and on any other grounds falling within* section 138(2)*,*
>
> *(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,*
>
> *(c) that the Secretary of State considers that –*
>
> *(i) each of the specified operational purposes (see* section 142*) is a purpose for which the examination of intercepted content or secondary data obtained under the warrant continues to be, or may be, necessary, and*
>
> *(ii) the examination of intercepted content or secondary data for each such purpose continues to be necessary on any of the grounds on which the Secretary of State considers that the warrant continues to be necessary, and*
>
> *(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.*"
>
> (ss.144, 163 and 185 of the Act)

68. As to modification, the provisions of bulk interception warrants, bulk acquisition warrants and bulk equipment interference warrants may be modified at any time in order to add, vary or remove any specified operational purpose or to provide that the warrant no longer requires or authorises specified activities: ss.145, 164 and 186. The addition or variation of a specified operational purpose is designated as a "*major*" modification, which is subject to a separate requirement for Judicial Commissioner approval (except in urgent cases, where Judicial Commissioner approval of a major modification must be sought and obtained within three working days): ss.145(5), 146-147; ss.164(5), 165-166; ss.186(6), 187-188.

69. As to cancellation, the Secretary of State (or a senior official acting on his/her behalf) may cancel a bulk interception warrant, bulk acquisition warrant or bulk equipment interference warrant at any time. Moreover, s/he must cancel such a warrant where certain conditions are met, *viz.* that the warrant is no longer necessary in the interests of national security[29], the conduct authorised by the warrant is no longer

[28] Save that in relation to an 'urgent' bulk equipment interference warrant (i.e. one issued without advance Judicial Commissioner approval: see above), the warrant ceases to have effect at the end of the period ending with the fifth working day after the day on which the warrant was issued.

[29] Save that this cancellation condition does not apply where the warrant has been modified so that it no longer authorises or requires: the interception of communications/obtaining of secondary data (in the case of a bulk interception warrant), the requiring of a telecommunications operator to disclose, or obtain and disclose, communications data specified in the warrant (in the case of a bulk acquisition warrant) or the securing of

proportionate to what is sought to be achieved by that conduct, or the examination of material obtained under the warrant is no longer necessary for any of the specified operational purposes (ss.148, 167, 189). Where a warrant is cancelled, the addressee of the warrant must, so far as reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible (ss.148(5), 167(5) 189(5)). A warrant that has been cancelled may not be renewed (ss.148(6), 167(6) and 189(6)).

III) TARGETED/THEMATIC EQUIPMENT INTERFERENCE WARRANTS UNDER PART 5

70. In addition to the bulk powers in Pt 6 Chs 1–3 of the Act, this claim concerns the lawfulness of aspects of the equipment interference regime in Part 5 of the Act.

71. The only aspects presently in issue are the provisions described in the Act as "*targeted equipment interference warrants*" (being warrants which authorise or require the addressee to secure interference with any equipment for the purpose of obtaining communications, equipment data or any other information (s.99(2)) where the subject matter of warrant falls within s.101(1)(b)-(h) of the Act (commonly referred to as "*thematic equipment interference warrants*")[30]:

> "*…(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*."

72. Several of the requirements for the issue of a targeted/thematic equipment interference warrant are similar to those that apply in relation to bulk warrants under Pt 6 Chs 1-3 (see above).

73. Thus, following an application made by an intelligence service, the Secretary of State may issue a targeted/thematic equipment interference warrant if:

---

interference with any equipment or the obtaining of any communications, equipment data or other information (in the case of a bulk equipment interference warrant): ss.148(4), 167(4) and 189(4).

[30] At this stage, Liberty does not ask the Court to rule on the lawfulness of a targeted examination warrant whose subject matter is as specified in s.101(1)(a) of the Act, i.e. "*equipment belonging to, used by or in the possession of a particular person or organisation*".

a. The Secretary of State considers that the warrant is necessary (i) in the interests of national security, (ii) for the purpose of preventing or detecting serious crime or (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 (s.102(1)(a) and (5)). A targeted/thematic warrant may be issued for any of these purposes.

b. The Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct (s.102(1)(b)).

c. The Secretary of State considers that satisfactory safeguards are in force in relation to the warrant pursuant to ss.129 and 130 (s.102(1)(c)). Those safeguards (concerning retention and disclosure of material, and the disclosure of material to overseas authorities) are essentially equivalent to those that apply in relation to bulk warrants, save that, given the 'non-bulk' nature of the material obtained under targeted equipment interference warrants, there is no process of 'selection for examination' of material obtained pursuant to a targeted equipment interference warrant, and therefore no 'examination safeguards' applicable to that process.[31]

d. Except in urgent cases, the decision to issue the warrant has been approved by a Judicial Commissioner (s.102(1)(d)). The provisions for Judicial Commissioner approval, and for retrospective approval or refusal in urgent cases, in ss.108-110 match those in relation to bulk equipment interference warrants (see above).

74. Additional safeguards apply where the purpose of an equipment interference warrant is to obtain items subject to legal privilege: s.112 of the Act. These mirror the safeguards applicable to the selection for examination of material obtained under a bulk warrant (see e.g. s.153 in relation to bulk interception warrants).

75. Further, where an application is made for a targeted equipment interference warrant and the purpose, or one of the purposes of the warrant, is to obtain confidential journalistic material or to identify / confirm a source of journalistic information, the application must contain a statement to that effect and a warrant may be issued only if specific arrangements are in place for the handling, retention, use and destruction of communications or other items of information containing such material: ss.113 – 114.

76. In contrast to the bulk powers, Part 5 of the Act also makes provision for the issue of targeted equipment interference warrants by the Scottish Ministers (s.103), by the Secretary of State to the Chief of Defence Intelligence (s.104) and by certain "*law enforcement chiefs*" to appropriate law enforcement officers (s.106-107). The requirements for the issue of warrants in these instances are similar, but not identical, to the requirements in s.102 of the Act (issue of a targeted equipment interference warrant by the Secretary of State to the head of an intelligence service).

[31] As with the bulk powers, there are also enhanced safeguards in relation to the retention of legally privileged material obtained pursuant to a targeted equipment interference warrant (s.131 of the Act).

77. S.115 of the Act makes detailed provision for, inter alia, the details that must be included in a targeted equipment interference warrant, which depends on the subject matter of the warrant. For instance, where the subject matter of such a warrant is equipment belonging to (etc.) persons who form a group which shares a common purpose or carries on a particular activity, the warrant must contain a description of the purpose / activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe: s.115(3).

78. Sections 116-125 make detailed provision for the duration, renewal, modification and cancellation of warrants (including targeted equipment interference warrants) issued under Pt 5 of the Act.

IV) BULK PERSONAL DATASET WARRANTS – PART 7

79. Under s.199(1) of the Act, an intelligence service retains a bulk personal dataset ("**BPD**") where: (a) it obtains a set of information that includes personal data relating to a number of individuals; (b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of intelligence interest; (c) after any initial examination[32] of the content, the intelligence service retains the set of information for purpose of the exercise of its functions; and (d) the set is held, or to be held, electronically for analysis in the exercise of those functions.[33]

80. An intelligence service may not exercise a power to retain a BPD unless its retention is authorised by either a "*class BPD warrant*" (authorising an intelligence service to retain, or retain and examine, any BPD of a class described in the warrant) or a "*specific BPD warrant*" (authorising an intelligence service to retain, or retain and examine, any BPD described in the warrant): s.200.

81. Part 7 does not itself contain any power to obtain a BPD. Rather, the requirement for a BPD warrant concerns the retention and any subsequent examination of a BPD obtained by other means. Such means may include a warrant issued under s.5 of the Intelligence Services Act 1994 ("**ISA**"), other exercise of the intelligence services' "information gateway" powers under the ISA and Security Service Act 1989, and the other powers under the Act (except for Pt 6 Ch 2).

82. In the case of both a class BPD warrant and a specific BPD warrant, the decision to issue must be taken by the Secretary of State personally: s.211.

83. The requirement for the authorisation of retention of a BPD by way of a warrant under s.200 does not apply where an intelligence service exercises a power to retain or examine a BPD obtained under a warrant or other authorisation issued or given under the 2016 Act itself: s.201(1). However, as discussed below, the Secretary of State may

[32] Section 220 provides for time limits on the initial examination of a set of information to determine whether it constitutes a BPD within the meaning of s.199 and, if so to seek a class or specific BPD warrant. Broadly speaking, the head of an intelligence service has 3 months to do so where the set of information was created in the UK, and 6 months where it was created outside the UK.

[33] "*Personal data*" means (a) data within the meaning of s.3(2) of the Data Protection Act 2018 (i.e. relating to an identified or identifiable living individual) which is subject to processing described in s.82(1) of that Act (processing by an intelligence service of personal data wholly or partly by automated means, etc.), or (b) data relating to a deceased individual which would fall within (a) if it related to a living individual.

direct that material so obtained should instead be treated as a BPD subject to the provisions of Pt 7.

(a) **Class BPD warrants**

84. On an application by the head of an intelligence service (or a person acting on his or her behalf), the Secretary of State may issue a class BPD warrant if (see s.204):

a. The Secretary of State considers that the warrant is necessary (i) in the interests of national security, or (ii) for the purposes of preventing or detecting serious crime, or (iii) in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security (s.204(3)(a));

b. The Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct (s.204(3)(b));

c. Where the warrant authorises the examination of BPDs of the class described in the warrant, the Secretary of State considers that (i) each of the specified operational purposes is a purpose for which the examination of BPDs of that class is or may be necessary, and (ii) the examination of BPDs of that class for each such purpose is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary (s.204(3)(c)(i) and (ii)). S.212 makes further provision for the specification of operational purposes in a warrant, in terms which mirror the provisions of s.142 of the Act in relation to bulk interception warrants and the equivalent provisions relating to bulk acquisition warrants and bulk equipment interference warrants.

d. The Secretary of State considers that the arrangements made by the intelligence service for storing BPDs of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory (s.204(3)(d)).

e. The decision to issue the warrant has been approved by a Judicial Commissioner (s.204(3)(e)). See s.208 for the provision as to Judicial Commissioner approval.

85. A BPD may not, however, be retained, or retained and examined, pursuant to a class BPD warrant if the head of the intelligence service considers that the BPD consists of

or includes, "*protected data*"[34] or "*health records*"[35] or that a substantial proportion of the BPD consists of "*sensitive personal data*"[36]: s.202(1) and (2).

86. Further, an intelligence service may not retain, or retain and examine, a BPD pursuant to a class BPD warrant if the head of the intelligence service considers that the nature of the BPD or the circumstances of its creation are such that its retention, or retention and examination, raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner on an application for a specific BPD warrant.

(b) **Specific BPD warrants**

87. A specific BPD warrant may be sought by the head of an intelligence service (or a person acting on his or her behalf) where (see s.205(1)-(3)):

    a. the BPD does not fall within a class described in a class BPD warrant; or

    b. The BPD falls within a class described in a class BPD warrant but the intelligence service is prevented from retaining, or retaining and examining, it in reliance on the class BPD warrant by virtue of the restrictions in s.202 (see above) *or* that intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.

88. Subject to those points, the basic criteria for the issue of a specific BPD warrant by the Secretary of State are the same as those for the issue of a class BPD warrant, save that advance Judicial Commissioner approval need not be obtained in urgent cases: see s.205(6)(a)-(e). Provision for *post hoc* Judicial Commissioner approval of specific BPD warrants in urgent cases is made at ss.209 – 210 (in terms which mirror the provision for such approval in relation to bulk equipment interference warrants in urgent cases).

89. Additional safeguards apply to applications for specific BPD warrants in relation to:

    a. Health records: Section 206(1)-(3) provides that the Secretary of State may only issue a specific BPD warrant the purpose (or one of the purposes) of which is to authorise the retention, or retention and examination, of health records in "*exceptional and compelling circumstances*". Section 206(4)–(5) provides that, where the head of an intelligence services considers that a BPD includes or is "*likely*" to include health records (but it is not a or the purpose

[34] Defined in s.203 as any data contained in a BPD other than systems data (see above), identifying data (see above) which is contained in the BPD which is capable of being logically separated from the BPD and if so separated would not reveal anything of what might reasonably be considered to be the meaning of the remaining data, and data which is not private information (which includes information relating to a person's private or family life).

[35] Defined in s.202(4) read with s.206(6) as a record, or copy of a record, which consists of information relating to the physical or mental health or condition of an individual, was made by or on behalf of a health professional in connection with that individual's care, and was obtained by the intelligence service from a health professional or a health service body (or from a person acting on their behalf).

[36] Meaning personal data consisting of information about an individual (whether living or deceased) or a kind mentioned in s.86(7)(a)-(e) of the Data Protection Act 2018 (covering matters such as personal data revealing political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation, and so on).

of a warrant to retain them), then the application must contain a statement to that effect.

b. Protected data: Section 207 provides that, where the Secretary of State decides to issue a specific BPD warrant, s/he may impose conditions which must be satisfied before "*protected data*" (see s.203, considered at fn 34 above) retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection.

(c) **Duration, renewal, modification and cancellation of BPD warrants**

90. Sections 213-219 make provision for the duration, renewal, modification and cancellation of BPD warrants. The provision made largely mirrors the provision for the duration, etc., of bulk warrants under Pt 6 Chs 1-3 (including the requirement for Judicial Commissioner approval of "*major modifications*").

91. One different provision is s.219, which provides that, where a BPD warrant ceases to have effect because it expires without having been renewed or is cancelled:

a. Within five working days after the expiry or cancellation of a BPD warrant, the head of the intelligence service to whom the warrant was addressed may either:

i. apply for a specific or class BPD warrant authorising the retention, or retention and examination, of the whole or any part of the material previously retained pursuant to a BPD warrant (in which case the usual criteria for the grant of such an application will apply) (s.219(2)(a)); or

ii. where the head of the intelligence service wishes to give further consideration to whether to apply for a further specific / class BPD warrant, apply to the Secretary of State for authorisation to retain / examine the whole or any part of the material retained in reliance on the warrant (s.219(2)(b)).

b. Where an application is made to the Secretary of State, s/he may direct that any of the material to which the application relates be destroyed (s.219(3)(a)), or (with the approval of a Judicial Commissioner) authorise the retention, or retention and examination, of any of that material, subject to such conditions as s/he considers appropriate, for a specified period not exceeding 3 months (s.219(3)(b)).

c. During that period, the head of an intelligence service may apply for a BPD warrant and must do so as soon as practicable and before the end of that period (s.219(7)).

d. S.219(8) provides that an intelligence service does not breach s.200 by virtue of its retention or examination of material to which a BPD warrant related

where that intelligence service is seeking a further warrant or authorisation pursuant to s.219 during the periods mentioned above, as follows:

i. "*First period*": Five working days from when the BPD warrant cases to have effect;

ii. "*Second period*": The period beginning with the day of any application under s.219(2)(a) or (b) and ending with its determination;

iii. "*Third period*": The period during which retention or examination is authorised under s.219(3)(b) (at most three months);

iv. "*Fourth period*": Where an authorisation under s.219(3)(b) is given and the head of an intelligence service then makes an application under s.219(7) for a BPD warrant, the period beginning with the expiry of the authorisation under s.219(3)(b) and the determination of the application.

(d) **Safeguards relating to the examination of BPDs**

92. S.221 requires the Secretary of State to ensure that arrangements are in force for securing that:

a. any selection for examination of data contained in BPDs is carried out only so far as is necessary for the operational purposes specified in the warrant (at the time of the selection); and

b. the selection of any such data is necessary and proportionate in all the circumstances.

93. The Secretary of State must also ensure, in relation to every specific BPD warrant in which conditions in relation to the selection for examination of data under s.207 (see above) are imposed, that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant.

94. As with the bulk powers in Pt 6 Chs 1-3, enhanced safeguards apply to the selection for examination pursuant to a specific BPD warrant of items subject to legal privilege (which differ depending on whether it is the / a purpose of the warrant to obtain privileged items, this is likely, or the addressee of a warrant considers that the data is not privileged because it or any underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose): s.222.

95. It is a criminal offence, punishable on conviction on indictment by a prison term of up to 2 years or an unlimited fine, to deliberately select data for examination under a class BPD warrant or a specific BPD warrant, knowing or believing that the selection of that data is in breach of certain specified safeguards (e.g. that any such selection is carried out only so far as is necessary for the operational purposes specified in the warrant, and so on): s.224.

(e) Application of Pt 7 to BPDs obtained under other powers in the Act

96. Section 225 provides that the Secretary of State may, on an application by the head of the intelligence service, give a direction that the intelligence service may retain, or retain and examine, a BPD that has been obtained under a warrant issued under another provision of the Act (except a bulk acquisition warrant under Pt 6 Ch 2). In such a case, the power under which the BPD was obtained ceases to apply, and the intelligence service thereafter requires the authorisation of either a class BPD warrant or a specific BPD warrant. Such a direction may provide for any "*associated regulatory provision*" specified in the direction to continue to apply in relation to the BPD (meaning any provision which is made by or for the purposes of the Act (other than Pt 7) that applied immediately prior to the direction). A direction under s.225 may only be given with the approval of a Judicial Commissioner, and it may not be revoked (it may be varied, but only for the purpose of altering or removing any provision included in the direction).

V) ACQUISITION AND RETENTION OF COMMUNICATIONS DATA – PTS 3 AND 4 OF THE ACT

97. Parts 3 and 4 of the Act were the subject matter of the February 2018 hearing. However, certain amendments to those Parts of the Act have taken effect since the Court gave its judgment in these proceedings on 27 April 2018.

98. Part 4 relates to the procedure for requiring telecommunications providers to *retain* communications data and Part 3 relates to the procedure for authorisation for relevant public authorities to *obtain* communications data. Those Parts of the Act are supplemented by the Communications Data Code of Practice (November 2018) (the "**CD CoP**"), which provides guidance on the procedures to be followed when acquisition of communications data takes place under Part 3 and when communications data is retained under Part 4.

(a) Retention of communications data – Part 4

99. Section 87 provides that the Secretary of State may, by notice (a "*retention notice*") require a telecommunications operator to retain relevant communications data if (a) the Secretary of State considers that the requirement is necessary and proportionate for one or more of the specified purposes and (b) the decision to give the notice has been approved by a Judicial Commissioner.

100. Since the Court's judgment in February 2018, the specified purposes (in s.87(1)) have been amended[37]. They are now restricted to retention that is necessary and proportionate: (i) in the interests of national security, (ii) for the applicable crime purpose (see s.87(10A)), 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

[37] By the Data Retention and Acquisition Regulations 2018 (SI 2018/1123, 1 November 2018).

damage to a person's physical or mental health, and (vi) to assist investigations into alleged miscarriages of justice. The crime purpose for which events data (such as call histories and location information) can be retained and acquired is restricted to 'serious crime', whereas entity data (such as the name of a subscriber to a service) can be obtained in relation to the full range of crimes. The provisions requiring approval of retention notices by a Judicial Commissioner have now come into force.[38]

101. As the Court noted in paragraphs [129] to [138] of its 27 April 2018 judgment:

    a. s.87(2) provides, *inter alia*, that a notice may relate to a "description of data", may relate to a particular operator or to a description of operators, and that a retention notice may specify the period of time for which data is to be retained, which may not exceed 12 months;

    b. before the Secretary of State may serve a retention notice, s/he must have regard to, among other matters, the factors listed in s.88(1), which comprise the likely benefits of serving the notice, the number of users to which the notice relates, the technical feasibility and costs of complying with the notice and any other effect on the telecommunications operator to be served;

    c. a retention notice may not be given unless the Secretary of State's decision has been approved by a Judicial Commissioner under s.89, requiring a review of whether the requirements in the proposed notice are necessary and proportionate, applying the same principles as would be applied in judicial review, and ensuring that his or her consideration is sufficiently careful so as to comply with the duties in s.2 of the Act;

    d. a telecommunications operator which receives a retention notice may refer the notice back to the Secretary of State for a formal process of review, in accordance with ss.90 to 91. These provisions are now fully in force and require the Secretary of State to consult and take into account the report of a Technical Advisory Board and a Judicial Commissioner (s.90(6), (9) and (10)). The Secretary of State may not vary or confirm a notice (as opposed to revoking a notice) unless that decision is approved by the IPC (s.90(11)).

(b) **Acquisition of communications data – Part 3**

102. Applications to *acquire* communications data can be authorised by three separate categories of individual, depending on the circumstances:

    a. s.60A of the Act confers power on the IPC to authorise applications for communications data in relation to the purposes set out in s.60A(7), i.e: (a) national security; (b) the applicable crime purpose (see s.60A(8)); (c) the economic well-being of the United Kingdom so far as relevant to the interests of national security; (d) public safety; (e) preventing death or injury or any

[38] Pursuant to reg. 4(a) of the Investigatory Powers Act 2016 (Commencement No. 7 and Transitional and Saving Provisions) Regulations 2018/873

damage to physical or mental health, or mitigating any injury or damage to physical or mental health; (f) assisting investigations into alleged miscarriages of justice, or (g) identifying dead or incapacitated persons;

b. s.61 provides for the authorisation of communications data requests relating to national security. Where an application for communications data is for the purpose of national security under s.61(7)(a), or economic well-being where relevant to national security under s.61(7)(c), or where it is an application made by a member of an intelligence agency under s.61(7)(b) (the applicable crime purpose), an application may, as an alternative to IPC authorisation under s.60A, be authorised internally by a designated senior officer in the public authority. The designated senior officer must, except where provided for in the Act, be independent of the operation concerned (see s.63(1));

c. s.61A provides for designated senior officers to grant authorisations in urgent cases. Examples of urgent circumstances, including an immediate threat of loss or serious harm to human life, an urgent operational requirement for data that will directly assist the prevention or detection of the commission of a serious crime or a credible and immediate threat to national security, are set out in CD CoP §5.31.

103. Under s.60A(1), the IPC may grant an authorisation, on an application made by a relevant public authority, where he considers that: (a) it is *necessary* for the relevant public authority to obtain communications data for a specified purpose falling within subsection 60A(7); (b) it is *necessary* for the relevant public authority to obtain the data (i) for the purposes of a specific investigation or a specific operation or (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data; and (c) that the conduct authorised by the authorisation is *proportionate* to what is sought to be achieved.

104. Similar conditions of necessity and proportionality apply for authorisations under s.61 and 61A (with the additional requirement of urgency in s.61A).

105. Ss.62-66 have been moved and grouped together under a new heading "*Further provision about authorisations*". They impose additional restrictions on acquisition of communications data, including:

a. Preventing local authorities from acquiring internet connection records for any purpose, and restricting the ability of other public authorities to access internet connection records to specific circumstances and purposes. This imposes a requirement for additional consideration of the proportionality of the application in relation to the level of processing and disclosure involved (see s.62 and CD CoP, Part 9);

b. Restricting the ability of designated senior officers to grant an authorisation if the officer is working on the relevant investigation or operation (s.63);

c. Specifying the content of authorisations (s.64);

d. Limiting the duration of authorisations (to one month, or 3 days in the case of urgent authorisations), subject to renewal or cancellation (s.65); and

e. Imposing duties on telecommunications providers, including a duty to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned (s.66).

106. Further safeguards are put in places by ss.76 and 77, in particular:

a. A requirement (subject to certain exceptions) to consult a person who is acting as a single point of contact in relation to the making of applications, before making any application to IPCO for authorisation under s.60A, or before a designated senior officer grants authorisation under s.61 or s.61A. Such consultation may encompass questions relating to the most appropriate methods for obtaining data, any unintended consequences of the proposed authorisation, and any issues as to the lawfulness of the proposed authorisation; and

b. A requirement for Judicial Commissioner approval for authorisations under s.61 or s.61A (or delegated decisions made under s.60A) to identify or confirm journalistic sources, where the authorisation is not necessary because of an imminent threat to life. S.77(6) requires, in particular, that the Judicial Commissioner must have regard to— (a) the public interest in protecting a source of journalistic information, and (b) the need for there to be another overriding public interest before a relevant public authority seeks to identify or confirm a source of journalistic information. This provision is supplemented by the CD CoP, §§8.23ff.

(c) RIPA Part 1 Chapter 2

107. The regime for the acquisition of communications data under Regulation of Investigatory Powers Act 2000 Pt 1 Ch 2 has not yet been repealed. It operates alongside IPA Pts 3–4 for some public authorities. The provisions have been amended to provide that "*traffic data*" and data about the use of any postal service, telecommunication service or part of a telecommunication system (see s.21(4)(a)-(b)) can only be acquired in relation to "*serious crime*".

VI) OVERSIGHT ARRANGEMENTS – PART 8 OF THE ACT

108. Part 8 makes provision for a series of oversight arrangements in relation to the exercise of the range of investigatory powers under the Act. In particular, Part 8:

a. provides for the appointment of a new IPC (the Investigatory Powers Commissioner) and other Judicial Commissioners; and

b. provides for the jurisdiction of the (existing) Investigatory Powers Tribunal ("**IPT**") in respect of the use of investigatory powers under the Act and introduces a new right of appeal against the IPT's decisions.

(a) **The IPC and the Judicial Commissioners**

109. The IPC replaces and consolidates the functions of a series of pre-existing oversight bodies, all of which were all abolished by the Act: s.240.

110. Section 227(1) requires the Prime Minister to appoint the IPC and such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the Judicial Commissioners' functions. The IPC and the Judicial Commissioners must hold or have held a high judicial office: s.227(2). The current (and first) IPC is the Rt Hon Lord Justice Fulford (appointed February 2017). His Deputy is the Rt Hon Sir John Goldring. The IPC is supported in his role by the Office of the Investigatory Powers Commissioner ("**IPCO**"). S.238 of the Act makes general provision for funding, staff and facilities in relation to the IPC and the Judicial Commissioners.

111. The IPC's main oversight functions are set out in s.229, and include (so far as is material):

    a. keeping under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to *inter alia* the interception of communications, the acquisition and retention of communications data and equipment interference: s.229(1)-(2);

    b. keeping under review (including by way of audit, inspection and investigation) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service: s.229(3)(a);

    c. keeping under review the operation of safeguards to protect privacy: s.229(5).

(i) Error reporting and notification to victims

112. Under s. 235(6) a public authority, telecommunications operator or postal operator must report to the IPC any "*relevant error*" (as defined in s. 231(9)). A "*relevant error*" means an error (a) by a public authority in complying with any requirements which are imposed on it by virtue of the Act or any other enactment and which are subject to review by a Judicial Commissioner and (b) of a description identified for this purpose in a code of practice specified under Schedule 7: s.231(9). The IPC must also keep under review the definition of "*relevant error*": s.231(9).

113. Under the Interception CoP §10.17, EI CoP §10.19, Bulk Acquisition CoP §10.15 and BPD CoP §8.11, relevant errors must be notified to the IPC "*as soon as reasonably practicable, and no later than ten working days after it has been established by appropriate internal governance processes that a relevant error has occurred*". Under CD CoP §24.26, the requirement is to report the error to the authority's senior responsible officer and then to the IPC "*within no more than five working days of it being established that an error has occurred*".

114. Under s.231(1) of the Act, the IPC must[39] inform a person of any "*relevant error*" relating to that person of which the Commissioner is aware if the Commissioner considers that (a) the error is a "*serious error*" and (b) it is in the public interest for the person to be informed of the error[40]. The IPC may not decide that an error is serious unless he considers that the error has caused significant prejudice or harm to the person concerned: s.231(2). The fact that there has been a breach of a person's Convention rights is not sufficient by itself to amount to a serious error: s.231(3).

115. When informing someone of an error, the IPC must also (s.231(6)):

> *"(a) inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and*
> *(b) provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to anything falling within subsection (4)(b)(i) to (iv)."*

(ii) Annual reporting by the IPC

116. The IPC must also, as soon as reasonably practicable after the end of each calendar year, make a report to the Prime Minister about the carrying out of the functions of the Judicial Commissioners (s.234(1)), including the detailed matters specified in s.234(2), which include statistics on the use of investigatory powers, information about the results and impact of such use, information about the operation of the safeguards under the Act, and so on. A report under s.234(1) must also include information about the number of relevant errors of which the IPC has become aware during the year to which the report relates, the number of such errors which the IPC has decided were serious errors, and the number of persons who have been informed of such errors: s.231(8).

117. On receipt of a report from the IPC under s.234(1), the Prime Minister must publish the report and lay a copy before Parliament: s.234(6)[41]. The IPC also has a discretion, where he considers it appropriate, to make a report to the Prime Minister on any matter relating to the functions of the Judicial Commissioners: s.234(4). A report under s.234(1) or (4) may, in particular, include such recommendations as the IPC considers appropriate about any matter relating to the functions of the Judicial Commissioners. The IPC is also required to make any report to the Prime Minister which the Prime Minister has requested: s.234(3).

(iii) Judicial Commissioners' functions

---

[39] Having first given the public authority which has made the error the opportunity to make submissions: s.231(5).

[40] In deciding this, the IPC must consider, in particular "*(a) the seriousness of the error and its effect on the person concerned, and (b) the extent to which disclosing the error would be contrary to the public interest or prejudicial to— (i) national security, (ii) the prevention or detection of serious crime, (iii) the economic well-being of the United Kingdom, or (iv) the continued discharge of the functions of any of the intelligence services*".

[41] S.231(7) provides that, on consultation with the IPC, the Prime Minister may exclude from the published version of the report any part of the report that would be contrary to the public interest or prejudicial to national security or other matters specified in s.231(7)(a)-(d).

118. The main relevant functions of Judicial Commissioners under the Act concern the giving of authorisations for warrants and notices issued by the Secretary of State in respect of the exercise of the various investigatory powers in the Act: see above. However, they also have a number of more general duties and powers under Part 8 of the Act.

119. Under s.229(6)-(7), when exercising functions under the Act, a Judicial Commissioner must not act in a way that s/he considers to be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime or the economic well-being of the United Kingdom, and must in particular ensure that the Commissioner does not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, or unduly impede the operational effectiveness of an intelligence service, police force, government department or Her Majesty's forces. However, these general duties do not apply in relation to certain of the Judicial Commissioners' functions, including deciding whether to approve the issue, modification or renewal of a warrant (s.229(8)(b)) and deciding whether to approve the grant, modification or renewal of a retention notice (s.229(8)(e)(i)).

120. Under s.235, the Judicial Commissioners have powers in relation to the carrying out of investigations, inspections and audits, including a power to obtain documents and information and to require assistance (including access to apparatus, systems, facilities and services) from "*relevant persons*", including any person who holds (or has held) an office, rank or position with a public authority and any telecommunications or postal operator who is, has been or may become subject to a requirement imposed by virtue of the Act (s.235(7)).

(b) **The IPT**

121. The Tribunal was established by s.65(1) of the Regulation of Investigatory Powers Act 2000 ("**RIPA**"). Members of the Tribunal must either hold or have held high judicial office or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

122. The Tribunal has exclusive jurisdiction to consider claims under s.7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss.65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

123. The Tribunal may also consider and determine any complaints by a person who is aggrieved by certain conduct[42] which s/he believes to have taken place (in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system, and to have taken place in "*challengeable circumstances*" or to have been carried out by or on behalf of the intelligence services (ss.65(2)(b), 65(4) of RIPA). Conduct takes place in "*challengeable circumstances*" when either it is the conduct of a public authority and it takes place

[42] A wide range of such conduct is specified in s.65(5) RIPA, and it includes the full panoply of actions that may be taken under the impugned parts of the 2016 Act.

with the (purported) authority of (inter alia) a warrant under Pts 5, 6 or 7 of the 2016 Act, an authorisation or notice under Pt 3 of the 2016 Act, or a retention notice under Pt 4 of the 2016 Act, *or* the circumstances are such that it would not have been appropriate for the conduct to take place without at least proper consideration having been given to whether such authority should be sought (RIPA, ss.65(7) and (8)).

124. Any person, regardless of nationality, may bring a complaint to the Tribunal. The IPT considered the scope of its jurisdiction and the extent of the knowledge or evidence of the use of investigatory powers required to make a claim in *Human Rights Watch v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib_15_165-CH.

125. Complaints are investigated and then determined by the Tribunal "*by applying the same principles as would be applied by a court on an application for judicial review*" (s.67(3) of RIPA). S.68(6) of RIPA gives the Tribunal powers to order production of materials by, among others, every person holding office under the Crown. Further, under s.232(1) of the 2016 Act, a Judicial Commissioner must give the IPT all such documents, information and other assistance as the IPT may require in connection with the investigation, consideration or determination of any matter.

126. Subject to any provision in its rules, the Tribunal may — at the conclusion of a claim — make any such award of compensation or other order as it thinks fit, including, but not limited to, an order quashing or cancelling warrants, authorisations, notices and directions given under the 2016 Act and an order requiring the destruction of any records of information which have been obtained in exercise of any power conferred by a warrant, authorisation or notice under the Act, or which are held by any public authority in relation to any person: s.67(7) of RIPA.

127. S.242 of the 2016 Act introduced a new s.67A of RIPA, which provided (for the first time) for a right of appeal on a point of law from final decisions of the IPT which are not procedural to the Court of Appeal. A decision of the Tribunal is subject to judicial review: *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22.