Appeal No UKSC/2018/0004

IN THE SUPREME COURT OF THE UNITED KINGDOM

ON APPEAL FROM HER MAJESTY'S COURT OF APPEAL (CIVIL DIVISION) (ENGLAND & WALES)

Neutral citation: [2017] EWCA Civ 1868; reported [2018] 1 WLR 2572

B E T W E E N:

R (PRIVACY INTERNATIONAL)

Appellant/Claimant

-and-

INVESTIGATORY POWERS TRIBUNAL

Respondent/Defendant

-and-

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

Interested Parties

CASE FOR LIBERTY

References in these submissions to the judgment of the Court of Appeal below ([2017] EWCA Civ 1868) take the form "CA [*x*]", where "*x*" is the paragraph number. These submissions have been updated (without substantive change) to reflect Liberty's permission to intervene granted on 6 November 2018.

A INTRODUCTION AND SUMMARY

1 This is the written case of The National Council for Civil Liberties ("**Liberty**"). Liberty applied to intervene in this appeal because of its experience in litigating important matters

of public interest before the Investigatory Powers Tribunal ("**IPT**" or "**the Tribunal**") and before the European Court of Human Rights ("**the Strasbourg Court**"), which is at present the only court in which decisions of the IPT may be challenged. Permission to intervene by written submissions and oral submissions limited to 30 minutes was granted by order of 6 November 2018.

2 Liberty's submissions may be summarised as follows:

(1) The jurisdiction of the IPT is very broad. Contrary to the impression given by the Court of Appeal, the jurisdiction of the IPT is not limited to reviewing the conduct of the Security Service, Secret Intelligence Services and Government Communications Headquarters ("**the intelligence services**"). It makes far-reaching determinations of law as to the compatibility of legislation with ECHR rights and with EU law. It also reviews surveillance (electronic or physical), the use of covert human intelligence sources, and other activities undertaken for policing, economic and other purposes by public authorities of a more mundane kind. These include police forces, HM Customs & Excise, the National Crime Agency, the Gambling Commission, the Department for Transport, the Home Office (for immigration enforcement), the Criminal Cases Review Commission, the Charity Commission, the Food Standards Agency, the Care Quality Commission, the Health and Safety Executive and the Competition and Markets Authority. It is objectionable in principle, and inimical to the rule of law, that a body with such broad jurisdiction should be entirely immune from challenge, save in the Strasbourg Court, and then only when the challenge raises a question of the UK's compliance with the ECHR.

(2) Even in relation to conduct of the intelligence services, there is (outside the IPT's narrowly circumscribed exclusive jurisdiction) considerable overlap between the jurisdiction of the IPT and that of the ordinary courts. If the Court of Appeal's construction is upheld, it will be a question of happenstance whether a determination on a particular issue will be entirely immune from review by the UK courts (as will be the case if the issue is determined by the IPT) or subject to appeal to the appellate courts and ultimately to this Court (as will be the case if the issue is determined by the ordinary courts). That it leads to such arbitrary consequences is a further reason to reject the Court of Appeal's construction of s. 68(7) of RIPA.

Authorities
Tab 1

(3) Contrary to the submission made to the Court of Appeal by the IPT itself, there is no practical or procedural difficulty in the High Court entertaining claims for judicial review of decisions of the IPT. Many of its decisions concern pure points of law. Where it is necessary for the High Court to consider material whose disclosure would be contrary to the public interest ("**sensitive material**"), there are mechanisms to permit that. In cases where disclosure would be contrary to the interests of national security, the Justice and Security Act 2013 ("**JSA**") empowers the High Court to hold a closed material procedure in which the sensitive material may be taken into account by the court. CPR Pt 82 contains detailed rules to ensure that such material is not disclosed contrary to the interest of national security. In any event, the Government has recently laid before Parliament in draft the Investigatory Powers Tribunal Rules 2018, which are closely modelled on CPR Pt 82. Once these rules come into force there will be no substantial difference between the procedure adopted in the High Court and that adopted in the IPT.

Authorities Tab 21

Authorities Tab 170

(4) In cases where the JSA does not apply (e.g. where disclosure would be contrary to a public interest other than national security), this Court's decision in *R (Haralambous) v Crown Court at St Albans* [2018] UKSC 1, [2018] AC 236 confirms that the High Court may still in principle hold a closed material procedure when hearing a claim for judicial review of a judicial body empowered to consider closed material. In cases where a closed material procedure is adopted, the High Court would no doubt exercise its inherent power to control its own procedure to ensure that sensitive material is not disclosed contrary to the public interest. If they were thought necessary, there would be nothing to prevent the making of procedural rules akin to those in CPR Pt 82.

Authorities Tab 21

Authorities Tab 94

Authorities Tab 170

B THE WIDE JURISDICTION OF THE IPT

3 The Court of Appeal's judgment gives the impression that the IPT is concerned exclusively with the security services and national security cases: **CA [42]**,[1] **[43]**,[2] **[46]-[48]**.[3] But that is not so.

Appendix pp. 19-21

4 The IPT:

(1) has wide-ranging jurisdiction over many subject matters and public authorities (only part of which is exclusive); and

(2) in consequence, decides many questions (including important questions of law) that have no particular relation to national security and which can and will arise in the ordinary courts.

5 The Court of Appeal wrongly ignored the full width of IPT's jurisdiction. This led it to describe the purpose of the Tribunal too narrowly. It also caused that Court to ignore the need for consistency between decisions of law of the IPT and the High Court. That consistency is achieved by allowing judicial review of IPT decisions.

(1) The IPT's jurisdiction and the limited extent to which it is exclusive

Authorities Tab 1

6 Annex A to this submission sets out RIPA s. 65, as it was in force prior to recent amendments.[4] However, for ease of exposition, Liberty summarises the heads of jurisdiction created by s. 65 in the table below:

---

1 "It is clear that Parliament's intention in establishing the IPT and in laying down a framework for the special procedural rules which it should follow, including the Rules, was to set up a tribunal capable of considering claims and complaints against the intelligence services under closed conditions which provided complete assurance that there would not be disclosure of sensitive confidential information about their activities."

2 "It would mean that despite the elaborate regime put in place to allow the IPT to determine claims against the intelligence services in a closed procedure while guaranteeing that sensitive information about their activities is not disclosed, judicial review proceedings could be brought in which no such guarantee applied."

Authorities Tab 6

3 In which the Court of Appeal considers *R (A) v Director of Establishments of the Security Service* [2010] 2 AC 1, a case concerning claims against the security services.

Authorities Tab 22

4 Amendments to RIPA by the Investigatory Powers Act 2016 were commenced as from March 2018, that is, after the decisions below and the application for judicial review in this case. Those amendments do not, however, alter the substance of the point below that the IPT retains a wide-ranging jurisdiction.

Head of jurisdiction	Exclusive to IPT?	Relevant provisions	
Claims under s. 7(1)(a) of the Human Rights Act 1998 ("**HRA**") for acts incompatible with Convention rights against the intelligence services or any other person in respect of (proposed) conduct by or on behalf of the intelligence services.	Yes	65(2)(a) and (3)(a)-(b)	Authorities Tab 16
Claims under s. 7(1)(a) of the HRA for acts incompatible with Convention rights brought by virtue of s. 55(4), which permits actions for damages for failure to ensure that encryption keys are held and dealt with appropriately.	Yes	65(2)(a) and (3)(c)	Authorities Tab 16 Tab 169 Tab 1
Claims under s. 7(1)(a) of the HRA for acts incompatible with Convention rights that relate to the taking place in "challengeable circumstances" of conduct falling within s. 65(5).	Yes	65(2)(a), (3)(d)	Authorities Tab 16 Tab 1
Conduct takes place in "challengeable circumstances" if it takes place with the (purported) authority of certain forms of authorisation or it would not have been appropriate for the conduct to take place without proper consideration having been given to whether such authority should be sought.[5] Those forms of authority are: an interception warrant (under s. 5);[6] an authorisation or notice under Part I Chapter II (retention and acquisition of communications data); an authorisation under Part II (for directed surveillance, intrusive surveillance, or the use/conduct of covert human intelligence sources); a notice under s. 49 (provision of encryption and other "keys" to access data);[7] an authorisation under s. 93 of the Police Act 1997 (to interfere with property); and RIPA s. 76A (authorisation of surveillance carried out by foreign police or customs officers in the UK).		65(7), (7ZA), (7A), (8)	Authorities Tab 1 Authorities Tab 169 Authorities Tab 15 Tab 169
Conduct falls within s. 65(5) if it is conduct:			
(i) by or on behalf of the intelligence services;		65(5)(a)	Authorities Tab 1
(ii) for or in connection with the interception of postal/electronic communications;		65(5)(b)	Authorities Tab 169 Tab 1
(iii) to which Chapter II of Part I (acquisition and disclosure of communications data) applies;		65(5)(c)	Authorities Tab 169 Tab 1
(iv) the carrying out of surveillance by a foreign police or customs officer (within the meaning of s. 76A);		65(5)(ca)	Authorities Tab 169 Tab 1
(v) other conduct to which Part II applies (directed surveillance, intrusive surveillance, or the use/conduct of covert human intelligence sources), but only if carried out by or on behalf of a person holding any office, rank or position with any of the intelligence services, Her Majesty's forces, any police force,		65(5)(d), (6)	Authorities Tab 169 Tab 1

5 Conduct authorised by or which takes place with the permission/authorisation of a "judicial authority" is not "challengeable conduct", save where the permission/authorisation is given under ss. 23A or 32A.

6 Or a warrant under the Interception of Communications Act 1985. Authorities Tab 12

7 And a permission under Schedule 2 (a permission to require the giving of a key for protected information).

the Police Investigations and Review Commissioner, the National Crime Agency, or the Commissioners for Her Majesty's Revenue and Customs; (vi) the giving of a notice under s. 49 (requiring provision of encryption and other "keys" to access data) or any disclosure or use of a key to protected information; or (vii) any entry on or interference with property or any interference with wireless telegraphy, but only if carried out by or on behalf of a person holding any office, rank or position with any of the intelligence services, Her Majesty's forces, any police force, the Police Investigations and Review Commissioner, the National Crime Agency, or the Commissioners for Her Majesty's Revenue and Customs.		65(5)(e) 65(5)(f), (6)	Authorities Tab 169 Tab 1 Authorities Tab 1
Complaints by a person aggrieved by conduct <u>falling within s. 65(5)</u>[8] and which <u>the person believes:</u> (i) to have taken place in relation to him, his property, any communications sent to/by him or intended for him, or his use of any postal/telecommunications service or telecommunications system; and (ii) to have taken place in "challengeable circumstances" (see above) or to have been carried out by or on behalf of any of the intelligence services.	No	65(2)(b) and (4)	Authorities Tab 1
Any reference by any person who has suffered detriment as a consequence of any prohibition or restriction by virtue of s. 17[9] on the person's relying in (or for the purposes of) any civil proceeding on any matter.	No	65(2)(c)	Authorities Tab 169

[8] The qualifications to s. 65(5)(d) and (f) that the conduct must be carried out by or on behalf of a person holding any office, rank or position with any of the intelligence services, Her Majesty's forces, any police force, the Police Investigations and Review Commissioner, the National Crime Agency, or the Commissioners for Her Majesty's Revenue and Customs do <u>not</u> apply for this purpose: see s. 65(6).

[9] Section 17 broadly speaking prohibits the suggestion or disclosure of lawful or unlawful surveillance having occurred. Specifically, subject to the exceptions in s. 18, s. 17(1) prevents any evidence, question, assertion, disclosure or other thing in/for/in connection with any legal proceedings that "(a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or (b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur." Section 17(2) lists: conduct by (broadly speaking) Ministers and civil servants, police force employees and postal/telecommunications employees that was or would be an offence under provisions preventing unlawful interception of communications; breach of the duty in s. 1(4) (to ensure that no request by a person in the UK for assistance in accordance with an international agreement providing for the interception of communications is made without lawful authority); issue of an interception warrant (under s. 5 or predecessor legislation); making an application for an interception warrant (or predecessor legislation); or imposing a requirement to provide assistance with giving effect to an interception warrant. Authorities Tab 169

7 Two important points emerge from this summary of the IPT's jurisdiction:

(1) The IPT has exclusive and non-exclusive jurisdiction over many different types of conduct of many public authorities beyond the intelligence services. This is because its jurisdiction is defined by reference to the nature of the legal claim, the nature of the authorisation given and/or the public authority in question. It is by no means limited to national security and the intelligence services.

(2) The IPT's jurisdiction is exclusive only for claims under s. 7(1)(a) of the HRA. This means that the IPT and the ordinary courts may be required to consider the same or related issues of law, both in claims against the intelligence services and other public authorities. As Lord Brown of Eaton-under-Heywood JSC said in *R (A) v Director of Establishments of the Security Service*: "subject always to the court's abuse of process jurisdiction and the exercise of its discretion in public law cases, proceedings outside section 7(1)(a) can still be brought in the courts".[10] This makes it a question of happenstance whether a determination on a particular issue will be entirely immune from review by the UK courts (as will be the case if the issue is determined by the IPT) or subject to appeal to the appellate courts and ultimately to this Court (as will be the case if the issue is determined by the ordinary courts).

Authorities Tab 16

Authorities Tab 6

(2) Types of conduct and bodies

8 As is apparent in particular from the jurisdiction conferred by RIPA s. 65(2)(a) and (3)(d) (the third head of jurisdiction in the table above), activities and public authorities to which the IPT's jurisdiction extends include notably:

Authorities Tab 1

(1) Acquisition and retention of communications data (under Part I Chapter II of RIPA),[11] by, for example, local authorities (such as any county or district council in England and London borough councils), police forces, the Gambling Commission, the Department for Transport, the Home Office (for immigration enforcement) and the Criminal Case Review Commission.[12] Under RIPA, acquisition of communications

Authorities Tab 169

---

10 *R (A) v Director of Establishments of the Security Service* [2009] UKSC 12, [2010] 2 AC 1 [33]. All other members of the Supreme Court agreed with Lord Brown.

Authorities Tab 6

11 RIPA s. 65(2)(a), (3)(d), (5)(c), (7), (8)(b).

Authorities Tab 1

12 RIPA s. 25(1) (definition of "relevant public authority") and Schedule 1; Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) Schedule 2.

Authorities Tab 169 Tab 19

data could be authorised if necessary: in the interests of national security; for the purpose of preventing or detecting all (not just serious) crime or disorder;[13] in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax, duty, levy or other imposition due to a government department; for the purpose, in an emergency, of preventing death, injury or damage to physical or mental health or mitigating any injury or damage to physical or mental health; to assist investigations into alleged miscarriages of justice; to identify persons who have died or are unable to identify themselves and to obtain information about their next of kin (or other connected persons) or reasons for death; and to exercise functions relating to the regulation of financial services and markets.[14] The 2016 Annual Report of the Interception of Communications Commissioner (Sir Stanley Burnton) explains that, of the 754,559 pieces of communications data acquired in 2016, 83% were for the purpose of preventing or detecting crime, 11% were for the purpose of preventing death or injury in an emergency, and 6% were for the purpose of national security.[15]

Authorities Tab 162

(2) Directed and intrusive surveillance and the use/conduct of covert human intelligence sources (under Part II of RIPA)[16] and surveillance by a foreign police or customs officer:[17]

(a) Directed surveillance and use of a covert human intelligence source may be authorised by public authorities including local authorities (such as any county or district council in England and London borough councils), police forces, various government departments (including the Department for Transport), the Charity Commission, the Food Standards Agency, the Care Quality Commission and the

---

[13] The failure to limit this purpose to serious crime was, however, ultimately held to be incompatible with EU law: *Secretary of State for the Home Department v Watson* [2018] EWCA Civ 70, [2018] QB 912 [9] (Lloyd-Jones LJ). The Divisional Court reached the same conclusion in relation to Parts 3 and 4 of the Investigatory Powers Act 2016, the successor communications data retention legislation, which suffered from the same vice: *R (The National Council for Civil Liberties) v Secretary of State for the Home Department* [2018] EWHC 975 (Admin) [30], [38], [186] (Singh LJ and Holgate J).

Authorities Tab 98

Authorities Tab 99

[14] RIPA s. 22(2); Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) Article 2.

Authorities Tab 169 Tab 19

[15] Interception of Communications Commissioner, *Annual Report for 2016* (December 2017, HC 297) 8.

Authorities Tab 162

[16] RIPA s. 65(2)(a), (3)(d), (5)(d), (7), (8)(c).

Authorities Tab 1

[17] RIPA s. 65(2)(a), (3)(d), (5)(ca), (7A).

Authorities Tab 1

Health and Safety Executive.[18] They may be authorised if necessary: in the interests of national security; for the purpose of preventing or detecting all (not just serious) crime or disorder; in the interests of the economic well-being of the United Kingdom; in the interests of public safety; for the purpose of protecting public health; and for the purpose of assessing or collecting any tax, duty, levy or other imposition due to a government department.[19]

(b) Intrusive surveillance may be authorised by police forces, the National Crime Agency, HM Revenue and Customs, a senior official by whom functions relating to immigration are exercisable, and the chair of the Competition and Markets Authority.[20] It may be authorised if necessary: in the interests of national security; for the purpose of preventing or detecting serious crime; or in the interests of the economic well-being of the United Kingdom.

(3) Entry onto or interference with property under s. 93 of the Police Act 1997, which may be authorised by police forces, the National Crime Agency, HM Revenue and Customs, a designated senior immigration officer, the CMA and the Police Investigations and Review Commissioner, for the purpose of preventing or detecting serious crime.[21] Authorities Tab 15

9 Cases the IPT has decided reflect its wide jurisdiction in terms of subject matter and public authorities. Its cases have included:

(1) *Paton v Poole Borough Council*, in which the IPT determined that the Council had carried out unlawful directed surveillance on a family purportedly under RIPA Part II. Council had carried out surveillance for three weeks to discover the complainant family's ordinary residence (which determined the appropriate school catchment area), so as to determine whether the complainant's mother had accurately stated it. Authorities Tab 140

---

18 RIPA s. 30(1) and Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) Schedule Part 1. The purposes for which particular public authorities may authorise these activities vary, but the point remains that their actions fall within the IPT's jurisdiction. Authorities Tab 169 Tab 20

19 RIPA ss. 28(3), 29(3). Authorities Tab 169

20 RIPA s. 32(6). Authorities Tab 169

21 Police Act 1997 s. 93(1), (2), (5).

The IPT held such surveillance was not for the purpose of the prevention and detection of crime and, further, was disproportionate in the circumstances.[22]

Authorities Tab 147 (2) *Chatwani v National Crime Authority*, where the IPT quashed an authorisation for property interference and the installation of covert listening devices in company premises controlled by the claimants.[23]

Authorities Tab 148 (3) *News Group Newspapers Ltd v Commissioner of the Police of the Metropolis*, where the police had authorised the acquisition of communications data to reveal journalistic sources about reports into the "Plebgate" affair. The IPT determined that three of the four authorisations made were necessary and proportionate, but one was not, and determined that the regime under RIPA s. 22 which applied at the time did not contain sufficient safeguards in relation to the protection of journalistic sources.[24]

Authorities Tab 169

Authorities Tab 139 (4) In *X v Local Authority*, the IPT determined that the installation of a hidden video camera by a local authority in order to obtain evidence identifying the person responsible for repeated dog fouling in the communal balcony area of council flats constituted directed surveillance for the purposes of RIPA.[25]

Authorities Tab 142 (5) In *B v Department for Social Development*, the IPT found that officers of the Northern Ireland Social Security Agency breached the complainants' rights under ECHR Article 8 by entering their house, posing as potential purchasers, and remaining on the property for 35 minutes during an investigation into allegedly overpaid benefits and allowances, without authorisation under RIPA.[26]

10 Further, several cases illustrate the potential jurisdictional overlap between questions of law that fall for decision by the IPT and the ordinary courts:

Authorities Tab 140 Tab 169 (1) In *Paton*, mentioned above, the Council contended that, if RIPA Part II did not provide the *vires* for its actions (as the IPT held), then s. 111 of the Local Government Act

---

Authorities Tab 140 [22] *Paton v Poole Borough Council* (IPT Case No IPT/09/01/C, 29 July 2010) [63], [68]-[69], [73].

Authorities Tab 147 [23] *Chatwani v National Crime Authority* [2015] UKIPTrib 15_84_88-CH (IPT Case No IPT/15/84/88/CH, 20 July 2015) [42].

Authorities Tab 148 [24] *News Group Newspapers Ltd v Commissioner of the Police of the Metropolis* [2015] UKIPTrib 14_176-H (IPT Case No IPT/14/176/H, 17 December 2015) [128]-[129].

Authorities Tab 139 [25] *X v Local Authority* (IPT Case No IPT/03/50/CH, 25 August 2008).

Authorities Tab 142 [26] *B v Department for Social Development* (IPT Case No IPT/09/11/C, 29 July 2011) [1], [22].

1972 did provide such power. (Section 111 stated relevantly that "a local authority shall have power to do any thing … which is calculated to facilitate, or is conducive to, the discharge of any of their functions".) The IPT did not ultimately need to decide the point, because it held that the conduct was disproportionate in any event.[27] But the interpretation and application of s. 111 of the Local Government Act is, of course, a matter that is frequently the subject of litigation in the ordinary courts.[28]

(2) In *AKJ v Commissioner of Police of the Metropolis*, the claimants brought claims against several chief constables in the High Court alleging that they had been had been deceived into engaging in intimate sexual relationships with undercover police officers. The Court of Appeal held that the conduct complained of fell within Part II of RIPA (so fell within RIPA s. 65(3)(d)) and in consequence: (1) claims that this was a breach of the claimants' Article 3 and 8 rights were within the IPT's exclusive jurisdiction (and were struck out);[29] but (2) claims in tort relating to exactly the same conduct were not within the IPT's jurisdiction at all and could proceed.[30] Whether the conduct was authorised under Part II of RIPA and proportionate would have been material to both parts of the claim, as lawful authority may have been a defence to the tort claims.[31]

Authorities Tab 80

Authorities Tab 169

Authorities Tab 1

(3) In *R (Butt) v Secretary of State for the Home Department*, where a claim that the collection and storage of data relating to the claimant was unauthorised directed surveillance under RIPA s. 26 was raised during the hearing, Ousley J held that such a complaint could have been brought before the Tribunal as "*the appropriate forum*", but that this did not mean it was the exclusive forum, and the High Court could determine that claim.[32]

Authorities Tab 92

Authorities Tab 169

---

27 *Paton v Poole Borough Council* (IPT Case No IPT/09/01/C, 29 July 2010) [77]-[78]. Authorities Tab 140

28 See, for example, the numerous authorities on the interpretation of s. 111 discussed in *Cross on Local Government Law* (2018) [1-25]-[1-36]. Authorities Tab 168

29 *AKJ v Commissioner of Police of the Metropolis* [2013] EWCA Civ 1342, [2014] 1 WLR 285 [41]-[43] (Lord Dyson MR). Authorities Tab 80

30 *Ibid* [51]-[52].

31 See *ibid* [49].

32 *R (Butt) v Secretary of State for the Home Department* [2017] EWHC 1930 (Admin), [2017] 4 WLR 154 [259]-[262] (Ousley J). Authorities Tab 92

11 This overlap of the legal issues that the IPT and High Court may decide demonstrates the desirability of the IPT's decisions on such points being amenable to judicial review (and, where appropriate, subsequent appeals) just as decisions of the ordinary courts on precisely the same points are subject to appeal.

(3) The IPT's jurisdiction to decide points of law of fundamental public importance concerning the powers of the intelligence services

12 The IPT regularly decides points of law of fundamental public importance, including these:

Authorities Tab 134 (1) In its second ruling in the *Kennedy* case, it held that "there is in public law no fundamental or basic common law right of privacy of communications attracting the principle of legality" and that irrationality, rather than proportionality, was the test for reviewing the lawfulness of the interception of communications at common law.[33]

Authorities Tab 135 (2) In *British-Irish Rights Watch v Security Service*, the IPT determined as a preliminary issue of law that the criteria under which telephone calls made from the UK to overseas telephones were intercepted and accessed were in accordance with the law for the purposes of Article 8 ECHR.[34]

Authorities Tab 143 (3) *Liberty v Government Communications Headquarters* concerned a challenge to various alleged programmes of the intelligence services following the Snowden disclosures.[35] The IPT dismissed challenges to the PRISM and UPSTREAM programmes and dismissed a claim that RIPA s. 8(4) was not in accordance with the law for the purposes of the ECHR. It further held that any indirect discrimination against non-UK nationals was justified and that there was no requirement under the ECHR for prior judicial authorisation for interceptions of journalists' communications. As a result of disclosures made in its first judgment, IPT held that the nature of the rules governing the acquisition of material from the United States under the PRISM and UPSTREAM programmes had not been sufficiently clear to comply with Article 8 of the ECHR until that judgment, but complied thereafter.[36]

Authorities Tab 134 [33] IPT Case No IPT/01/62, 9 December 2004 [33](2)-(3).

Authorities Tab 135 [34] *British-Irish Rights Watch v Security Service* (IPT Case No IPT/01/77, 9 December 2004) [39].

Authorities Tab 143 [35] *Liberty v Government Communications Headquarters* [2014] UKIPTrib 13_77-H, [2015] 3 All ER 142 [140], [148], [151] (*Liberty/Privacy (No 1)*).

[36] *Ibid* [55], [153]-[155].

(4) In *Lucas v Security Service*, the IPT considered the legality of the Wilson doctrine, a policy limiting the interception of MPs' telephone communications.[37] It held that the doctrine was not absolute and did not apply to warrants under RIPA s. 8(4) but only to the targeted interception or accessing of MPs' communications. It held the doctrine itself had no legal effect and was not enforceable by way of legitimate expectation. It further held the regime for the interception of MPs' communications was compatible with Article 8 of the ECHR.

Authorities Tab 149

Authorities Tab 169

(5) *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* concerned the acquisition and use by the intelligence services of bulk personal and bulk communications datasets.[38] The IPT held that it was lawful for the Secretary of State to issue notices under Telecommunications Act 1984 s. 94 requiring provision of bulk communications data to the Secretary of State, notwithstanding the enactment of RIPA Part I Chapter II (which provided expressly for the retention by telecommunications operators and acquisition by government bodies of communications data).[39] It also held that this regime was incompatible with Article 8 ECHR until March 2015 when it was revealed but thereafter compatible.[40] The IPT subsequently referred[41] to the CJEU questions as to whether the intelligence services' activities fall within the scope of EU law and are subject to the e-Privacy Directive or to the CJEU's decision in *Watson*.[42] The CJEU has yet to deliver its ruling. The IPT later ruled (by a majority) that the regime for sharing bulk data with foreign agencies complied with Article 8 ECHR and (unanimously) that various directions under the 1984 Act had not been in accordance with the law and that sharing of bulk data with law enforcement agencies and industry partners complied with UK law and the ECHR.[43]

Authorities Tab 150

Authorities Tab 169

Authorities Tab 151

Authorities Tab 107

Authorities Tab 153

---

37 *Lucas v Security Service* [2015] UKIPTrib 14_79-CH, [2017] 1 All ER 283, [17], [23], [32]. Authorities Tab 149

38 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib 15_110-CH, [2016] HRLR 21 (October 2016). Authorities Tab 150

39 *Ibid* [27], [41], [57].

40 *Ibid* [83]-[84], [100]-[101].

41 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2017] UKIPTrib IPT_15_110_CH (8 September 2017) [72]. Authorities Tab 151

42 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Watson* [2017] QB 771. Authorities Tab 107

43 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2018] UKIPTrib IPT_15_110_CH (23 July 2018) [47], [77], [86]. Authorities Tab 153

Appendix pp. 48-102

(6) The instant case concerned the question whether the respondents' assumed computer network exploitation, *i.e.* hacking, was lawful. The IPT decided the majority of preliminary legal issues in favour of the respondents, including questions about the effect of the Computer Misuse Act 1990, the construction of the Intelligence Services Act 1994 and the compatibility of the regime with the ECHR.[44]

13 The effect of the Court of Appeal's judgment in the present case is that the IPT's decisions on these and other similar points of fundamental public importance are challengeable only in the Strasbourg Court — and then only when the challenge raises an issue as to the UK's compliance with the ECHR. This means that:

(1) There is no opportunity for rulings on the interpretation of domestic legislation, or on the common law, to be considered by the UK appellate courts, including this Court, unless they happen to arise in other litigation brought in the ordinary courts.

(2) The only way of challenging rulings adverse to the complainant dealing with the compatibility of domestic conduct or legislation with the ECHR is by applying directly to the Strasbourg Court. This means that, on subjects of fundamental importance, the IPT alone represents the UK in the important "dialogue" between the Strasbourg court and the national courts.[45] This is inappropriate because, however eminent its president and members may be, the IPT does not have the collective judicial experience or status of the appellate courts of England and Wales, Scotland and Northern Ireland, or of this Court.

(3) Where the IPT's rulings are adverse to the government, there is no means at all of challenging them.

14 These consequences tell strongly against the Court of Appeal's construction of RIPA s. 68(7).

Authorities Tab 1

Appendix p. 48 [44] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib 14_85-CH (12 February 2016).

Authorities Tab 82 [45] See, eg, *R (Nicklinson) v Ministry of Justice* [2014] UKSC 38, [2015] AC 657 [117] (Lord Neuberger).

C NO DIFFICULTY IN DEALING WITH SENSITIVE MATERIAL IN ORDINARY COURTS

15 The Court of Appeal repeatedly emphasised the so-called "particular sensitivity in relation to the evidential material in issue and the public interests which may be jeopardised if it is disclosed"[46] in cases before the IPT. Unusually, the IPT itself played an active part in the proceedings below: it provided a note that "pointed out the practical difficulties which would arise in judicial review proceedings in relation to handling of sensitive confidential information if this court concludes that … the IPT is amenable to judicial review".[47] Appendix pp. 128-149

16 Liberty submits that these and similar concerns are misplaced for two reasons:

(1) First, in many cases, the questions decided by the IPT are questions of law, including, but not limited to, questions as to the compatibility of legislation with Convention rights. Claims for judicial review of such questions are unlikely to give rise to the need to consider sensitive material.

(2) Secondly, to the extent that such a need does arise, it is adequately catered for by closed material proceedings under the Justice and Security Act 2013 in the context of national security and, otherwise (or in any event), the principle explained in *R (Haralambous) v Crown Court at St Albans*.[48] Authorities Tab 94

17 Accordingly, these concerns are not a reason that supports the construction of RIPA s. 67(8) adopted below. Authorities Tab 1

(1) Concern overstated by Court of Appeal

18 The IPT has developed the practice of holding open hearings to determine points of law on assumed facts. The hearing in the present case provides an example. The question of the required specificity of a warrant under s. 5(2) of the Intelligence Services Act 1994 is a pure point of law. The IPT's generous interpretation to the intelligence services[49] in its open judgment is troubling. There is no reason — let alone good reason — that this Authorities Tab 14

---

46 CA [7], [12]. Appendix pp. 12, 13

47 CA [4]. Appendix p. 4

48 [2018] UKSC 1, [2018] AC 236. Authorities Tab 94

49 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib 14_85-CH (12 February 2016) [45]-[47]. Appendix p. 77

decision should not be subject to judicial review and appeal from the judicial review decision in the ordinary way. No special procedure would be needed. The same is true of judicial review proceedings to challenge the legal determinations set out in paragraph 12 above.

(2) In any event, the ordinary courts have, and always had, proper mechanisms to deal with sensitive material

19 Even where it is necessary to place sensitive material before the High Court on a claim for judicial review of an IPT decision, the High Court has powers and may adopt appropriate procedures to ensure that sensitive material is not disclosed. These are the powers and procedures:

(1) under the JSA, where there is a national security reason for non-disclosure; and

(2) otherwise (or in addition), those that exist by necessary implication from the statutory power of the body below to consider sensitive material.

(a) JSA: Closed material proceedings in the ordinary courts in national security cases

Authorities Tab 21 20 The JSA enables the ordinary courts to invoke a closed material procedure in national security cases. The provisions are modelled on those that have applied in SIAC since 1997. Their effect is to provide a bespoke mechanism for dealing with sensitive material of precisely the kind considered by the IPT in the national security context.

Authorities Tab 170 21 In summary, as implemented by CPR Pt 82, the JSA has the effect that:

(1) The High Court, Court of Appeal or this Court (and the equivalent courts in Scotland and Northern Ireland) may declare that a closed material application may be made in civil proceedings where:

(a) a party would (leaving aside questions of public interest immunity, voluntary decisions not to disclose and prohibitions on disclosure) be required to disclose "sensitive material" (s. 6(4)), that is, "material the disclosure of which would be damaging to the interests of national security" (s. 6(11)); and

Authorities Tab 21

(b) "it is in the interests of the fair and effective administration of justice in the proceedings to make a declaration" (s. 6(5)).

Authorities Tab 21

The proceedings thereby become "section 6 proceedings", that is, proceedings in which a closed material application may be made.

(2) Once a declaration is made under s. 6, a party may make a "closed material application" to the Court for permission to disclose sensitive material only to the Court and/or any Special Advocate acting for a party (s. 8(1)(a), CPR rr. 82.1(2)(b) and 82.3(2)). Where a closed material application is made, the Attorney General must be informed (CPR r. 82.9(1)) and may appoint a Special Advocate to represent the interests of a party who is excluded from part of the proceedings (s. 9(1)). As explained below, before closed material may be relied upon, a Special Advocate must be appointed (CPR r. 82.13).

Authorities Tab 21

Authorities Tabs 21 & 170

Authorities Tab 170

Authorities Tab 21

Authorities Tab 170

22 For such proceedings, CPR rr. 82.2(1)-(2) provide that the overriding objective must be read and given effect in a way that is compatible with the duty to "ensure that information is not disclosed in a way which would be damaging to the interests of national security."

Authorities Tab 170

23 Relevant provisions in CPR Pt 82, which serve the same purpose as the IPT procedural regime discussed by the Court of Appeal (**CA [42]-[44], [48]**), include the following:

Appendix pp. 19-21

(1) A party must apply for permission to withhold sensitive material and may not rely upon sensitive material at a hearing on notice unless a Special Advocate has been appointed to represent the interests of the party to whom it is not disclosed (CPR r. 82.13). However, by CPR r. 82.14(10): "The court must give permission to the relevant person to withhold sensitive material where it considers that disclosure of that material would be damaging to the interests of national security" (emphasis added).

Authorities Tab 170

(2) The court must exclude a party and its legal representative from (part of) a hearing where this is "necessary … in order to secure that information is not disclosed where disclosure would be damaging to the interests of national security" (CPR r. 82.6(1)).

Authorities Tab 170

(3) A Special Advocate may not communicate with the party whose interests they represent after the sensitive material is served on the Special Advocate unless she or he obtains a direction from the Court permitting a proposed communication, which must itself be given to the Court and to the Secretary of State and on which they may make submissions (CPR r. 82.11).

Authorities Tab 170

(4) If the Court gives permission to withhold sensitive material, it must consider whether to direct that an open summary of that material be served, but it "must ensure that any such summary does not contain material the disclosure of which would be damaging to the interests of national security" (CPR r. 82.14(7)).

Authorities Tab 170

(5) If the Court refuses permission to withhold sensitive material, or directs a summary to be served, the material still need not be disclosed/the summary need not be served (CPR r. 82.14(9)). Instead, if the Court considers that the material undermines the non-disclosing party's case, the Court may direct that certain points not be taken or concessions be made and, otherwise, may direct that the non-disclosing party not rely on the material. Therefore the Government retains the discretion not to disclose sensitive material, even where the Court considers that it could be disclosed or summarised without damaging national security.

Authorities Tab 170

(6) To the extent it is necessary to include in reasons material whose disclosure would be damaging to national security, the Court is to include those reasons in a separate, closed judgment, which is shown only to the government and the Special Advocate (CPR r. 82.16).

Authorities Tab 170

Authorities Tab 23

24 The draft Investigatory Power Tribunal Rules 2018, laid before Parliament in October 2018 after extensive public consultation, will (if affirmed) further narrow any existing differences between the procedure adopted in the IPT and that adopted by the ordinary courts under the JSA when dealing with sensitive material. They include:

(1) a general duty on the Tribunal to endeavour, subject to its duty to secure that information is not disclosed contrary to the public interest, to conduct proceedings, including any hearing, in public and in the presence of the complainant;[50] and

(2) an express power in the Tribunal to direct disclosure, but (as under the JSA) subject to the caveat that, if the respondent elects not to disclose, the Tribunal may direct the respondent not to rely on particular points, make concessions or take other steps.[51]

Authorities Tab 23

[50] Rule 10(4).

[51] Rule 7.

25 These new Rules make it impossible to contend that there are any substantial or important differences between the IPT's procedure and that of the ordinary courts under the JSA. Liberty proposes to address in oral argument any submissions to the contrary that are raised by the IPT (again) or the Interested Parties. Authorities Tab 23

(b) Outside the scope of the JSA: implied power to hold closed proceedings on judicial review

26 To the extent the JSA does not apply (for example because disclosure would be contrary to a public interest other than national security), a court hearing a claim for judicial review of a decision of a court or tribunal expressly authorised to consider sensitive material may still hold a closed material procedure: *R (Haralambous) v Crown Court at St Albans*.[52] Authorities Tab 94

27 As Lord Mance said: "the only sensible conclusion is that judicial review can and must accommodate a closed material procedure, where that is the procedure which Parliament has authorised in the lower court or tribunal whose decision is under review".[53] As he explained, the power to do so arises by necessary implication from the statute that permits such a procedure by the original decision-making body, given Parliament's understanding of the importance of judicial review. Lord Mance added "that, even before judicial review was regulated by statutory underpinning[54], I would also have considered that parallel considerations pointed strongly to a conclusion that the present situation falls outside the scope of the principle in *Al Rawi* and that a closed material procedure would have been permissible on a purely common law judicial review".[55] Authorities Tab 72

28 It follows from *Haralambous* that the Court of Appeal was wrong to hold that: Authorities Tab 94

(1) "the ordinary courts do not have general powers to conduct examination of claims in closed proceedings from which an individual claimant is excluded" and such powers were conferred only later by the JSA, in the context of judicial review (**CA [9]**); and Appendix p. 12

(2) permitting judicial review of IPT decisions would subvert the "elaborate regime" created by RIPA s. 67(8) and the Tribunal's Rules to ensure that "there would not be disclosure of sensitive confidential information about [the intelligence services'] Authorities Tabs 1 & 2

---

52 [2018] UKSC 1, [2018] AC 236. Authorities Tab 94

53 See at [59]. Authorities Tab 94

54 This refers to the provisions for judicial review in s. 31 of the Senior Courts Act 1981: see *ibid* [56]-[58]. Authorities Tabs 11 & 94

55 See at [59]. Authorities Tab 94

Appendix p. 19

activities", because such information may be revealed on judicial review (**CA [42]-[43]**), or would "permit the special procedural regime established for the IPT to be bypassed at the stage when judicial review proceedings in respect of its decisions are brought in the High Court" (**CA [48]**).

Appendix p. 21

Authorities Tab 94

29 In fact, *Haralambous* makes clear that judicial review of decisions of a body able to consider closed material (such as the IPT) must, and before the JSA was enacted always could, accommodate closed material proceedings if necessary. There is no reason why the procedures that the High Court applies in closed proceedings under the implied jurisdiction recognised by *Haralambous* would be more likely to result in the disclosure of sensitive information than the IPT's own closed proceedings or closed proceedings under the JSA.[56]

30 If it were thought necessary to do so, there would be nothing to preventing the making of procedural rules akin to those in CPR Pt 82 governing the exercise of this implied jurisdiction. It may be noted, however, that the Government, in its response to the consultation on the draft IPT Rules, rejected a suggestion that specific rules should be made governing closed material procedures in appeals from the IPT (once provision is made to bring the right of appeal into force). In the Government's view, such rules were not needed because "[c]losed material procedures would, in principle, be available and the Civil Procedure Rules do not need to be amended to facilitate this". This is presumably because the Government (rightly) recognises the ability of the courts to devise and operate closed material procedures appropriate to the nature of the decision under review.

Authorities Tab 170

Authorities Tab 167

(c) Would Parliament in 2000 have assumed that judicial review courts could not entertain closed material?

31 The JSA was enacted in 2013. But it does not follow that Parliament, when enacting RIPA in 2000, would have assumed that judicial review of a body specifically empowered to consider sensitive material would have been impossible. In 2000:

(1) There was by that time a well-established line of case law in which the courts had entertained judicial review proceedings challenging decisions that relied on sensitive

Authorities Tab 170

[56] If rules of court analogous to CPR Pt 82 were considered necessary, these could be made. For example, CPR Pt 82 could be amended so as to apply to any closed proceeding (as well as those under the JSA).

material, where necessary by applying the presumption of regularity: see eg *R v Inland Revenue Commissioners, ex parte Rossminster* [1980] AC 592. Authorities Tab 47

(2) The suggestion that the courts might at common law develop closed material procedures (forestalled by the Supreme Court's decision in *Al Rawi v Security Service*[57]) could hardly have been ruled out. As Lord Dyson pointed out,[58] the availability of a closed material procedure at common law had been assumed in a series of cases (by judges as eminent as Lord Woolf MR and Sir Anthony Clarke MR). When the point was fully argued, directly, in *Al Rawi*, the first instance judge (Silber J) held that a closed material procedure was available.[59] Authorities Tab 72 Authorities Tab 69

32 There is, accordingly, no proper basis to assume that Parliament would, even in 2000, have regarded it as procedurally or practically impossible for a judicial review court to entertain a challenge to the decision of a court or tribunal empowered to receive sensitive closed evidence with appropriate protection for that sensitive material (*contra* **CA [8]-[12]**). This substantially undermines the Court of Appeal's conclusion (**CA [12]**) that "the procedural regime governing the IPT and its differences from that applicable to the ordinary courts at the time RIPA was enacted are significant features of the legal context in which s 67(8) of RIPA falls to be construed". Appendix pp. 12-13 Appendix p. 13

D CONCLUSION

33 The Court is respectfully invited to take note of the above submissions in determining this appeal.

MARTIN CHAMBERLAIN Q.C.

DAVID HEATON

19 October 2018 (updated 12 November 2018)

---

57 [2011] UKSC 34, [2012] 1 AC 531. Authorities Tab 72

58 *Ibid* [51]-[58].

59 *Al Rawi v Security Service* [2009] EWHC 2959 (QB) [91]-[92]. Authorities Tab 69