Reemers Publishing Services GmbH
O:/Beck/Dietrich_Sule/3d/Part 5.3d from 25.03.2019 16:33:27
3B2 9.1.580; Page size: 160.00mm × 240.00mm

Chapter 3
Intelligence Law and Oversight in the UK

Outline

Bibliography: Aldrich, R., "Whitehall and the Iraq War: the UK's Four Intelligence Enquiries" *Irish Studies in International Affairs*, 16 (2005), 73–88; R. Aldich, GCHQ: the uncensored story of Britain's most secret intelligence agency (Harper Collins, 2011); R. Aldrich and R. Cormac, *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (Harper Collins, 2016); Anderson D., *Report of the Bulk Powers Review*, Cm. 9326 (2016); Andrew, C., *Secret Service: the Making of the British Intelligence Community* London, 1986; Andrew, C., *Defence of the Realm: the Authorized History of MI5* (London, 2009); Birkinshaw, P., *Reforming the Secret State* (Milton Keynes, 1990); Bochel, H., Defty, A., Kirkpatrick, J., *"New mechanisms of independent accountability: select committees and Parliamentary scrutiny of the intelligence services"* Parliamentary Affairs, 68 (2) 314–331 (2015); Born, H., L, Johnson and I. Leigh, *Who's Watching the Spies: Establishing Intelligence Service Accountability* Dulles, Virginia, 2005; Born, H. and I. Leigh, "Democratic Accountability of Intelligence Services", *Armaments, Disarmament and International Security, Yearbook of the Stockholm International Peace Research Institute 2007*, (Oxford University Press 2007), ch. 5; Born, H., Leigh, I. and Willss A., *International Intelligence Cooperation and Accountability* London Routledge, 2011; Born, H., Leigh, I. and Willss A., *Making International Intelligence Cooperation Accountable* Oslo, Norwegian Parliament Printing House, 2015; Chamberlain, M., "Update on procedural fairness in closed proceedings". (2009) 28(4) Civil Justice Quarterly 448–543; Davies, P., *MI6 and the Machinery of Spying* (Frank Cass, 2004); Defty, A., "Educating parliamentarians about intelligence: The role of the British Intelligence and Security Committee" *Parliamentary Affairs* 2008 61(4):621–641; Fikfak, V. and H. Hooper, *Parliament's Secret War* (Hart, Oxford 2018); Forcese, C. and L., Waldman, *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of "Special Advocates" in National Security Proceedings* Ottawa, 2007; Gill P., *Policing Politics: Security Intelligence and the Liberal Democratic State*, (Frank Cass, London, 1994); Forsyth, C., "Public Interest Immunity: Recent and Future Developments" (1997) 56 *Cambridge Law Journal* 51; Gill, P.,"The Politicization of Intelligence: Lessons from the Invasion of Iraq", in H. Born, L.

Johnson and I. Leigh (eds.), *Who's Watching the Spies: Establishing Intelligence Service Accountability* Dulles, Potomac Books, 2005; Gill, P., "Evaluating Intelligence Oversight Committees: the case of the UK Intelligence Security Committee and the "War on Terror"" Intelligence and National Security, 22(1) pp. 14–37 (2007); Gill, P., "The ISC and the Challenge of International Security Networks", Review of International Studies 35 (2009) p. 932; Glees, A., P. Davies, P. and J. Morrison, *The Open Side of Secrecy: Britain's Intelligence and Security Committee*, London., Social Affairs Unit, 2006; Glover, R., *Murphy on Evidence* (14th ed., Oxford 2015), ch. 13; Horne, A. and Walker, C., "Parliament and National Security" in Horne, A. and Le Sueur, A. (eds.), P*arliament: Legislation and Accountability* (Hart, Oxford, 2016); Intelligence and Security Committee, *Iraqi Weapons of Mass Destruction- Intelligence and Assessments*, Cm.5972, 2003; Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and Transparent Legal Framework* (March 2015) HC 1075; Jackson, J.,"The Role of Special Advocates: Advocacy, Due Process and the Adversarial Tradition", (2016) 20(4) International Journal of Evidence and Proof 343–362; Jacob, J.,"From Privileged Crown to Interested Public" [1993] *Public Law* 121; Jeffery, K., *MI6: the History of the Secret Intelligence Service 1909–1949* (Bloomsbury, 2010); Justice, *Secret Evidence* London, 2009; Leigh, I., "Public Interest Immunity", (1997) *Parliamentary Affairs* 55–70; Leigh, I., and L. L. Lustgarten, "Five Volumes in Search of Accountability: The Scott Report", (1996) 59 *Modern Law Review* 695–725; Leigh, I., Reforming Public Interest Immunity [1995] 2 Web Journal of Current Legal Issues http://www.bailii.org/uk/other/journals/WebJCLI/1995/issue2/leigh2.html; Leigh, I.,"Parliamentary Oversight of Intelligence in the UK: A Critical Evaluation" in H. Born and M. Caparini (eds.), *Democratic Control of Intelligence Services: Containing Rogue Elephants* Aldershot, Ashgate, 2007; Leigh, I.,"The Role of Judges" in S. Farson and M.Pythian (eds.), *Commissions of Inquiry and National Security: Comparative Approaches* (Praeger, 2010), ch. 16; Leigh, I.,"National Courts and International Intelligence Cooperation" in H. Born, I. Leigh and A. Wills (eds.), *International Intelligence Cooperation and Accountability*, (Routledge, 2011); Leigh, I., "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade After 9/11" (2012) 27 (5) Intelligence and National Security 721–737; Lustgarten, L. and I. Leigh *In From the Cold: National Security and Parliamentary Democracy*, Oxford, Oxford University Press, 1994; McKay, S., Blackstone's Guide to the Investigatory Powers Act 2016 (Oxford University Press, Oxford, 2017); McKay, S. and Walker, C., "Legal regulation of intelligence services in the United Kingdom" in Dietrich, J-H. and Eiffler, S.R. (eds.), *Handbuch des Rechts der Nachrichtendienste* (Richard Boorberg, Stuttgart, 2017); Moran, J. and Walker, C., "Intelligence Powers and Accountability in the U.K." in Goldman, Z.K. and Rascoff, S.J. (eds.), Global Intelligence Oversight: Governing Security in the Twenty-First Century (Oxford University Press, New York, 2016) pp. 289–314; Murray C., "Out of the Shadows: the Courts and the United Kingdom's Malfunctioning Counter-Terrorism Partnerships", *Journal of Conflict & Security Law* 2013, 18(2), 193–232; Peto, A. and Tyrie, A., *Neither Just Nor Secure* London Centre for Policy Studies, 2011; Phythian M., "The British Experience with Intelligence Accountability" *Intelligence and National Security*, 22 (1), p. 81 (2007); Pythian, M.,"Intelligence Oversight in the UK: The case of Iraq", in L. Johnson (ed.), *Handbook of Intelligence Studies*, (Routledge 2007); Phythian M.,"A Very British Institution": The Intelligence and Security Committee and Intelligence Accountability in the United Kingdom', in Loch K. Johnson (ed.), *Oxford Handbook of National Security Intelligence* (New York, Oxford University Press, 2010), 699–718; Phythian, M., "The British Experience with Intelligence Accountability: The First Twenty Years", in Loch K. Johnson (ed.) *Essentials of Strategic Intelligence* (Santa Barbara, CA, Praeger Security International, 2015), 447–69; Sullivan, J., "Closed Material Procedures and the Right to a Fair Trial" , 29 *Maryland J. Int'l Law* 269 (2014); Supperstone, M., "A New Approach to Public Interest Immunity?" [1997] *Public Law* 211; Tomkins, A.,"Public Interest Immunity After Matrix Churchill" [1993] *Public Law* 650; Tomkins, A.,"National Security and the Due Process of Law" 64(1) *Current Legal Problems* 215–253 (2011); Wadham, J., "The Intelligence Services Act 1994" *Modern Law Review,* 57: 916–927 (1994).

A. Introduction

1 This Chapter addresses the legal framework within which security and intelligence agencies operate in the United Kingdom. A brief historical sketch traces the agencies from their foundation in the early twentieth century, focusing particularly on controversies since the end of the Cold War. This is followed by discussion of the legal basis and the role of the intelligence agencies, as well as the non-statutory elements of the intelligence community. The succeeding section deals with the powers of the agencies. This area which has undergone extensive discussion following the disclosures since 2013

of Edward Snowden and comprehensive revision, especially of bulk collection powers, in new legislation- the Investigatory Powers Act 2016.

Discussion of the accountability and oversight arrangements for the agencies falls under three headings: ministerial responsibility and control; parliamentary oversight through the Intelligence and Security Committee; and judicial oversight by the Commissioners (and the newly-created office of the Investigatory Powers Commissioner) and by the body responsible for handling complaints concerning the agencies (the Investigatory Powers Tribunal). **2**

The section examining intelligence and the courts opens by discussing how far the historically deferential attitude of the judiciary towards claims of national security has been modified post 9/11. It then moves on to assess evidential and procedural restrictions designed to allow and protect intelligence in civil proceedings: Public Interest Immunity, followed by the growth in use of security-cleared Special Advocates and the introduction of Closed Material Procedures. **3**

The Conclusion points to some emerging and future trends, notably the increasing importance of cyberwarfare and the future of intelligence cooperation after Brexit.

B. A historical sketch

I. Origins of the security and intelligence agencies

The United Kingdom does not have a written constitution. Historically, matters of defence and national security were dealt with under powers derived from the prerogative (the residue of non-statutory power enjoyed by Crown and recognised at common law). This includes decisions over war and peace, the deployment of armed forces and the creation and organisation of security forces. In modern times these prerogative powers are exercised by ministers on behalf of the Crown rather than by the sovereign personally. Elements of control outside the executive branch have been introduced as a number of aspects of the defence and security prerogatives have been replaced or limited by legislation. In addition, the reach of judicial review by the courts into this field has extended in recent years and increasingly Parliament also has sought to call the government to account for the exercise of security and defence powers. **4**

The three main security and intelligence agencies were created secretly in the early twentieth century, without reference to Parliament, under prerogative powers. The Secret Service Bureau, the forerunner of both MI5 and MI6 dated from 1909.[1] The predecessor of GCHQ, the Government Code and Cipher School, was established in 1919.[2] Official acknowledgement of their existence and the granting of statutory charters came much later: to the Security Service (MI5) in 1989 and to the Secret Intelligence Service (SIS or MI6) and the Government Communications Headquarters (GCHQ) in 1994. The relevant statutes are the Security Service Act 1989 and the Intelligence Services Act 1994 (the latter covering SIS and GCHQ). **5**

Prior to the 1989 legislation the Security Service's work was governed by the Maxwell-Fyfe Directive – a brief administrative Charter named after the Home Secretary who issued it in 1952 – which emphasized the Service's role in the "Defence of the **6**

[1] C. Andrew, *Secret Service: the Making of the British Intelligence Community* (London 1986) 121 ff.; C. Andrew, *Defence of the Realm: the Authorized History of MI5* (London, 2009) S. A, Chs. 1–3.

[2] https://www.gchq.gov.uk/topics/our-history (accessed 6 June 2018).

Realm", together with its duty to behave non-politically.[3] The Service was, nevertheless, responsible to the Home Secretary and its Director-General had a right of access to the Prime Minister. The Security Service Act 1989 reaffirmed the existing constitutional position under the Directive and gave an explicit statutory basis for the Service's work. The impetus for doing so came from concerns that the Service's use of surveillance and personal information violated the right to private life, home and correspondence under the European Convention on Human Rights.

7 GCHQ (Government Communications Headquarters)[4] – the signals intelligence agency – came to public attention in the mid-1980s, largely because of a protracted industrial dispute about the ban on officers there belonging to a trade union[5] and disclosures about war-time code-breaking, but it lacked a statutory remit until 1994. The Secret Intelligence Service (MI6) was not even officially acknowledged to exist until 1992.[6] The Intelligence Services Act 1994 provided a statutory charter for both agencies and it also filled notable gap in the 1989 Act by creating for all the three agencies a statutory committee of parliamentarians, drawn from both Houses of Parliament -the Intelligence and Security Committee ("ISC"). The Justice and Security Act 2013 formally reconstituted the ISC as a committee of Parliament, although there remain some differences between it and a conventional parliamentary select committee. It is the current legislation governing its remit and powers.

II. Recent controversies

8 The agencies have been drawn into controversy on several occasions following 9/11, partly as alleged failures relating to the intelligence leading up to Iraq war and prior to major terrorist attacks in Britain. Allegations about complicity in torture or rendition have been extensively litigated and are under continuing investigation by the Intelligence and Security Committee. Finally, the disclosures of Edward Snowden have resulted in a flurry of legal challenges by NGOs to various surveillance practices, several major reviews of surveillance and to a comprehensive new statutory regime (the Investigatory Powers Act 2016).

9 The events prior to the Iraq War raised serious public concerns that the possible politicisation of intelligence. The government chose, in the attempt to enlist public and political support for its policy, to release, in September 2002 and February 2003, two dossiers of intelligence-related material concerning the attempts of the Iraqi regime to acquire and develop "Weapons of Mass Destruction".[7] Allegations that intelligence was fabricated or knowingly mis-stated for political ends were subsequently refuted following official reports by the Intelligence and Security Committee (ISC) and by Lord Hutton, a senior judge. They did, however, find other unsatisfactory features concerning

[3] *Lord Denning's Report*, Cmnd. 2152 (1963); https://www.mi5.gov.uk/who-we-are (accessed 6 June 2018).

[4] https://www.gchq.gov.uk/topics/our-history (accessed 6 June 2018). On the history of GCHQ see R. Aldich, GCHQ: the uncensored story of Britain's most secret intelligence agency (Harper Collins, 2011).

[5] The decision was unsuccessfully challenged in the courts: *Council of Civil Service Unions v. Minister for the Civil Service* [1985] AC 374.

[6] http://www.mi6.gov.uk/output/sis-home-welcome.html. An official history of the early decades of SIS was published in 2010: K. Jeffery, MI6: the History of the Secret Intelligence Service 1909–1949 (Bloomsbury, 2010). See also P. Davies, MI6 and the Machinery of Spying (Frank Cass, 2004).

[7] P. Gill, "The Politicization of Intelligence: Lessons from the Invasion of Iraq", in H. Born, L. Johnson and I. Leigh (eds.), *Who's Watching the Spies: Establishing Intelligence Service Accountability* (Dulles, Virginia, 2005). M. Pythian, "Intelligence Oversight in the UK: The case of Iraq", in L. Johnson (ed.), Handbook of Intelligence Studies, (Routledge 2007).

the process. The ISC criticised the prominence given to one claim (that Saddam Hussein possessed weapons of mass destruction that could be brought into use in 45 minutes) and the partial and misleading treatment given to it.[8] The subsequent Hutton report found that the Joint Intelligence Committee Chairman and staff may have been "subconsciously" influenced to make statements that were more definitive than was usual in intelligence assessments in compiling the dossiers with a view to publication.[9] A later Privy Counsellors' review chaired, by Lord Butler (a former Cabinet Secretary),[10] confirmed this conclusion and went further in proposing safeguards over future public uses of intelligence and in suggesting changes in MI6, Defence Intelligence and JIC practice. These resulted in two reforms to the central intelligence machine. The first was the combining of the roles of Secretary to the Joint Intelligence Committee and Intelligence Coordinator into a Permanent Secretary of Intelligence, Security and Resilience whose responsibilities now also include giving strategic guidance to the intelligence community and accounting for the resources devoted to the agencies under the Single Intelligence Account. The second was the creation within the Cabinet Office of the post of Professional Head of Intelligence Analysis.[11]

Allegations of complicity by UK agencies in the torture of terrorist suspects held abroad led to investigations by the Intelligence and Security Committee (the "ISC") in 2007 into extraordinary renditions[12] and by the Parliamentary Joint Committee on Human Rights in 2009.[13] In a legal challenge brought by one Guantanamo Bay detainee, Binyam Mohammed, the Court of Appeal found in 2010 that the Security Service had misled the ISC that they "operated a culture that respected human rights and that coercive interrogation techniques were alien to the services' general ethics methodology and training". In contrast, Lord Neuberger concluded, that "at least some Security Services officials appear to have a dubious record when it comes to actual involvement and frankness about such involvement with the mistreatment of Mr Mohamed".[14] Following the judgment the government settled the claim and those brought by a number of other litigants, who claimed that the agencies had been complicit in torture, by paying substantial compensation. Detailed instructions to cover the questioning by the agencies of terrorist suspects held abroad were published[15] and a judicial inquiry was established. The inquiry was subsequently disbanded, however, in the light of fresh criminal investigations into the involvement of MI6 in the rendition to Libya of a dissident, Abdel Hakim Belhaj, and his wife, Fatima Boudchar, which came to light after the fall of the Gaddafi regime, as it was unable to complete its work while the criminal investigations were in progress. In December 2013 the ISC agreed to take over the

10

[8] Intelligence and Security Committee, *Iraqi Weapons of Mass Destruction- Intelligence and Assessments*, Cm. 5972, 2003, para 86.

[9] *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly C.M.G.,* H.C. 247 (2003–4), para 467, http://www.the-hutton-inquiry.org.uk.

[10] *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Counsellors* (2003–4) HC 898.

[11] *National Intelligence Machinery* 2010.

[12] Intelligence and Security Committee, Rendition (2007), Cm 7171, paras 111–47. See also: Intelligence and Security Committee, The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq (2005) Cm 6469.

[13] Joint Committee on Human Rights, Allegations of UK Complicity in Torture, para 60.

[14] *R (on the application of Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 158, para 29.

[15] Consolidated Guidance to Intelligence Officers and Service Personnel on Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62632/Consolidated_Guidance_November_2011.pdf (accessed 21 February 2018).

investigation from the judicial inquiry and this work is ongoing. In May 2018 the Prime Minister made a formal apology to Belhaj and Boudchar for the UK Government's actions.[16]

11 The Snowden revelations have had a significant impact in the UK since a number of them concern the work of GCHQ and its collaboration with the NSA in bulk collection of communication data. Snowden's allegations made the public aware about the agencies collection activities on a previously unimagined scale. Those alleged activities include, among other things, the services' direct access to fibre optic cables that carry much communications traffic (TEMPORA),[17] access to the servers of leading internet companies under joint programmes (PRISM),[18] and extensive computer network exploitation to implant malware (in particular to access Belgacom and Gemalto, a major producer of mobile phone SIM cards).[19]

12 The UK Government's initial reaction was to issue categorical- if carefully worded- denials of Snowden's allegations that SIGINT cooperation is used to circumvent legislation. In Parliament Ministers' initial response to Snowden's allegations was a mixture of generalised reassurance and to point to the more detailed, but largely irrelevant, scheme governing interception warrants. Since the allegations centred on "mass surveillance" by GCHQ involving interception of external communications and collection of metadata this amounted to evasion rather than a meaningful response. The ISC supported these ministerial assurances by its own statement on the PRISM programme[20] that it had found no evidence that the law was being broken. Far from being an endorsement of the existing position, if anything these statements implied that the legislation was deficient, as the committee itself later acknowledged in its 2015 report *Privacy and Security*.[21]

13 There followed a spate of other official reviews and test cases brought by privacy campaigners (described in S. D. II below). The outcome is that a number of obscure or secret information-gathering techniques employed by the agencies, particularly in relation to bulk data and equipment interference, have been officially acknowledged and brought within a detailed statutory framework.

14 The Investigatory Powers Act 2016 makes significant changes to the legal regime governing surveillance (see S. D. III-VI below).[22] Some of these changes (especially

[16] "Belhaj Rendition: UK apology over Libyan dissident treatment", BBC News 10 May 2018. http://www.bbc.co.uk/news/uk-44070304 (accessed 5 June 2018).

[17] TEMPORA was said to involve the interception by GCHQ of digital traffic flowing through the underwater fibre optic cables landing in the UK.

[18] "The PRISM programme was said to involve the collection by the NSA of data from the servers of nine US internet companies (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple –'*the Prism Providers*'). Types of data collected included a range of digital information such as email, chat, videos, photos, stored data, VOIP, video conferencing and online social networking details." (Anderson, *A Question of Trust*, Annex 7).

[19] David Anderson QC (Independent Reviewer of Terrorism Legislation), *A Question of Trust*, Annex 7.7.

[20] Statement by the ISC regarding GCHQ's alleged access to the US PRISM programme, July 2103 https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717_ISC_statement_GCHQ.pdf?attachauth=ANoY7coZE-rHTq9Qzt2ZUBDHYRhsr1oop0VRWbG3M7vS0R8jGCov-CwsUInaAlJ4T05hWcB8ApdN3mbge3Ey66211zyzdHjeyIj1x_pScLmjavzvy-4Dsxp4MojNPfJGRvSlAbi–oOL2cFrLrIz6SqlaQ5n4yc1sAJzUNhv54EHYePW7mN5742OVbKTsdSXfzc7g_Id8cv_a-fVJhyzy2xCAu-QiXORftFftP-kzkMNH8sujSgGNIsTQ%3D&attredirects=0.

[21] Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and Transparent Legal Framework* (March 2015) HC 1075.

[22] The legislation is highly technical and complex and only a brief summary of the relevant key features can be given here. See further: S. McKay, Blackstone's Guide to the Investigatory Powers Act 2016 (Oxford University Press, Oxford, 2017).

those on data retention, precipitated by the *Digital Rights* judgment)[23] had been under discussion for several years and had already generated significant opposition from civil libertarians, prior to the Snowden revelations. Nonetheless, it is clear that those disclosures had a significant impact, in particular by forcing additional admissions about bulk collection or strategic communication intelligence by UK agencies, by fuelling a debate about the legality and the adequacy of oversight of these practices within the current regime, and by shaping proposals in the draft legislation.[24]

C. The legal basis for and role of the intelligence agencies

The relevant provisions are the Security Service Act 1989[25] and the Intelligence Services Act 1994 (the latter covering SIS and GCHQ). Other parts of the intelligence machinery – especially those concerned with intelligence analysis- such as the Defence Intelligence and the Joint Intelligence Committee are creatures of the prerogative and remain outside the statutory framework. A separation is made between security and policing: the agencies do not have the power to arrest or to prosecute- even in the fields of counter-terrorism and counter-espionage, these are the province of the police and the Crown Prosecution Service, with whom the services work closely. **15**

Before the 1989 Act the Security Service's work was governed by the Maxwell-Fyfe Directive – a brief administrative Charter named after the Home Secretary who issued it in 1952 – which emphasized the Service's role in the "Defence of the Realm", together with its duty to behave non-politically.[26] The Service was, nevertheless, responsible to the Home Secretary and its Director-General had a right of access to the Prime Minister. The Security Service Act 1989 reaffirmed the existing constitutional position under the Directive (the Service was accountable only to ministers and not to Parliament) but cast it in statutory form. However, the Act did provide an explicit statutory basis for the Service's work. The impetus for doing so came from concerns that the Service's use of surveillance and personal information violated the European Convention on Human Rights (see further below). **16**

GCHQ (Government Communications Headquarters)[27] – the signals intelligence agency – came to public attention in the mid-1980s, largely because of a protracted industrial dispute about the ban on officers there belonging to a trade union[28] and disclosures about war-time code-breaking, but it lacked a statutory remit until 1994. **17**

[23] Emergency legislation was introduced (the Data Retention and Investigatory Powers Act 2014) following the judgment of the CJEU in *Digital Rights Ireland Ltd v. Minister for Communications* (Joined Cases C 293/12 and C 594/12) to provide a stop-gap legal basis for requirements on telephone and internet companies to retain "communications data" on individuals for up to a year. This legislation contained a sunset clause of 31 December 2016 and is superseded by the Investigatory Powers Act 2016, Pt. 3.

[24] Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and Transparent Legal Framework* (March 2015) HC 1075 (hereafter *"Privacy and Security"*); David Anderson QC (Independent Reviewer of Terrorism Legislation), *A Question of Trust: Report of the Investigatory Powers Review* (2015) (hereafter *"A Question of Trust"*) ; Royal United Services Institute, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (London, 2015) (hereafter *"A Democratic Licence to Operate"*) .

[25] I. Leigh and L. L. Lustgarten, "The Security Service Act 1989" (1989) 52 *Modern Law Review* 801–836; P. Birkinshaw, *Reforming the Secret State* (Milton Keynes, 1990).

[26] See also http://www.mi5.gov.uk//history.html.

[27] https://www.gchq.gov.uk/(accessed 6 June 2018).

[28] The decision was unsuccessfully challenged in the courts: *Council of Civil Service Unions v. Minister for the Civil Service* [1985] AC 374.

The Secret Intelligence Service (MI6) was not even officially acknowledged to exist until 1992.[29] The Intelligence Services Act 1994 provided a statutory charter for both agencies and it also filled notable gap in the 1989 Act by creating for all three agencies a statutory committee of parliamentarians, drawn from both Houses of Parliament -the Intelligence and Security Committee.[30]

18 Although MI5 is a security agency, MI6 is responsible for intelligence[31] and GCHQ for signals intelligence and information security,[32] all three agencies have the common statutory functions of the protection of national security, protecting the economic well-being of the UK[33] and assisting (the police or customs) in preventing or detecting serious crime. The statutory approach to national security differs markedly, however, between the Security Service and the other agencies. This is undoubtedly because of civil liberties sensitivities about the impact of domestic security operations, although strictly the legislation does not prohibit domestic operations against appropriate targets by SIS and GCHQ (nor prohibit MI5 from working overseas).

19 Consequently the Security Service's statutory aims are more closely defined than with the other agencies: in its case the protection of national security, including (but not limited to) protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and "actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means" ("counter-subversion").[34] The breadth of these aims reflects the Cold War origins of the Maxwell-Fyfe Directive. In practice, however, counter-terrorism now accounts for more than 80 % of MI5's effort and resources. Since the end of the Cold War the controversial area of counter-subversion, which many believed betrayed a bias against radical political and pressure groups, has been dormant.[35] In view of the politically sensitive nature of its role in the domestic arena, there are two important safeguards that limit the Service's work.[36] Collection of information must be restricted to what is "necessary for the proper discharge of its functions" (and likewise its disclosure). The Director-General is also responsible for ensuring that the Service does not take any action to further the interests of any political party.

20 The Intelligence Services Act takes a much broader approach to SIS and GCHQ-referring to "the interests of national security, with particular reference to the Defence and foreign policies of Her Majesty's Government".[37] The emphasis on the policies of the government of the day, rather than on overriding national interests is an oblique acknowledgement that the priorities of these agencies are set through "tasking" approved at ministerial level in the annual submission "United Kingdom's National Requirements for Secret Intelligence".

21 Within these broad parameters the functions of MI6 are "to obtain and provide information relating to the actions or intentions of persons outside the British Islands.

[29] http://www.mi6.gov.uk/output/sis-home-welcome.html.

[30] L. Lustgarten and I. Leigh, In From the Cold: *National Security and Parliamentary Democracy* (Oxford 1994), Coda; J.Wadham, "The Intelligence Services Act 1994" (1994) 57 *Modern Law Review,* 916–927.

[31] http://www.mi6.gov.uk/output/sis-home-welcome.html.

[32] http://www.gchq.gov.uk/.

[33] Limited, however, to the actions or intentions of persons outside the British Islands.

[34] Security Service Act 1989, S. 1.

[35] Lustgarten and Leigh, In From the Cold, Ch. 14.

[36] Security Service Act 1989, S. 2(2).

[37] Intelligence Services Act 1994 Ss. 1(2)(a) and 3(2)(a). GCHQ's functions can also be exercised under Ss. 3(2) "in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands;" and "in support of the prevention or detection of serious crime".

[and] …to perform other tasks relating to the actions or intentions of such persons".[38] The coy reference to other "other tasks" is of course polite usage for a range of actions from espionage to covert action, many of which will be illegal according to the laws of the country where they are undertaken.

GCHQ has two roles: signals intelligence and information assurance. In relation to **22**
the first its brief to conduct all types of signals interception (and disruption) and decryption.[39] The second (and more defensive) role is that of providing technical advice on communications and information technology security to government departments and the armed forces.[40] A significant omission is the failure of the 1994 legislation to detail the arrangements for international cooperation (especially with the United States' National Security Agency, the NSA) which is known to affect much of GCHQ's work.

Four parts of the intelligence structure are outside the statutory framework – the **23**
Defence Intelligence, the Joint Intelligence Committee (JIC), the Intelligence Assessments Staff and the Joint Terrorism Analysis Centre (JTAC).[41] The role of the first two especially came under close scrutiny as a result of events surrounding the use of intelligence in the public justification of the UK's involvement in the war in Iraq. The Defence Intelligence[42] is part of the Ministry of Defence and supports the Armed Forces by analyzing information, from open and covert sources, and providing assessments both for them and for the Joint Intelligence Committee. It provides assessments and advice to guide policy decisions, inform defence research and equipment programmes; and support military operations. The head, the Chief of Defence Intelligence (who reports to the Minister of Defence) is also responsible for coordination of intelligence throughout the Armed Forces. The Joint Intelligence Committee sits at the hub of the intelligence machine, in the Cabinet Office, formally connecting it with government. It is responsible for tasking the agencies (especially SIS and GCHQ) and for providing intelligence assessments based on the agencies' output which are circulated within government, including the relevant ministers. The JIC membership includes not only the heads of the security and intelligence agencies, but also senior officials from the Cabinet Office, the Foreign Office, the Ministry of Defence, the Home Office, the Department of Trade and Industry and the Treasury. The Joint Terrorism Analysis Centre (JTAC) was created in 2003 as the UK's centre for the analysis and assessment of international terrorism. It is housed within the Security Service (since this the lead agency for counter-terrorism in the UK) and is responsible to the Director-General of the Service.[43] Its role is to analyse and assess all intelligence relating to international terrorism, whether domestic or abroad, and to produce threat assessments to other government departments and agencies. JTAC's effectiveness is monitored by an Oversight Board, chaired by the Cabinet Office.

[38] Intelligence Services Act 1994, S. 1(1).

[39] "to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material": Intelligence Services Act 1994, S. 3 (1) (a).

[40] S. 3 (1) (b).

[41] *National Intelligence Machinery* 2010.

[42] Formerly the Defence Intelligence Staff. For a current description of Defence Intelligence see: https://www.gov.uk/government/groups/defence-intelligence (accessed 6 June 2018).

[43] Ibid., 15.

D. The powers of the agencies

I. Introductory

24 The agencies powers are limited to information gathering through various means related to their function.[44] They do not have powers of arrest or detention and formal powers to question or interview individuals. The Security Service in particular, however, works closely with the police in counter-terrorism and official secrets investigations and prosecutions.[45]

25 The origins of the power to intercept communications in the UK are obscure: up to the 1980s the government relied on the prerogative as legal authority for warrants issued by ministers for mail opening and phone tapping, until the practice was successfully challenged before the European Court of Human Rights in the *Malone* case.[46] Following that decision a statutory scheme for interceptions was enacted-initially in the Interception of Communications Act 1985 and then in the Regulation of Investigatory Powers Act 2000.[47] This permits warrants (still issued by a minister, rather than a judge) for the prevention or detection of serious crime, in the interest of national security or for safeguarding the country's economic well-being. The system is overseen by a Judicial Commissioner who reports annually. The Investigatory Powers Act 2016 (not yet in force) introduces important changes to this system of "targeted surveillance" by the agencies, described below.

26 The need to demonstrate a clear legal basis for other forms of state surveillance in order to comply with Article 8 also led in 2000 to the introduction of an umbrella regime for covert surveillance by the services and the police – the Regulation of Investigatory Powers Act 2000. The 2000 Act currently governs intelligence gathering by the agencies involving the use of covert surveillance, covert human intelligence sources (agents) and various forms of technical surveillance: the interception of communications, and the acquisition, disclosure and retention of communications data. The legislation requires that intelligence gathering using any of these must be authorised by designated persons within the agencies who review that it is necessary and proportionate to the aims of the investigation, and that the information cannot be obtained using less intrusive methods.[48] These authorisations must be recorded, and made available for review by the Judicial Commissioners, who ensure intelligence gathering is proportionate and not used excessively or inappropriately. Interception of communications and "intrusive surveillance" (i. e. conducted on private premises or a private vehicle) additionally require a warrant signed by a Secretary of State. Many instances of

[44] General provisions apply. S. 2(2) of the Security Service Act 1989 requires the Director-General to ensure that there are arrangements limiting the collection of information by that Service to that necessary for the proper discharge of the Service's role or for preventing or detecting serious crime. There are equivalent provisions for MI6 and GCHQ: Intelligence Services Act 1994, Ss. 2(2)(a) and 4(2)(a).

[45] On police powers of surveillance see M. Amos "The Impact of Human Rights Law on Measures of Mass Surveillance in the United Kingdom", in F. Davis, N. McGarrity and G. Williams, Surveillance, Counter-Terrorism and Comparative Constitutionalism (Routledge, 2014).

[46] *Malone v. UK* (1984) 7 EHRR 14.

[47] For an overview see: J. Moran and C. Walker, "Intelligence Powers and Accountability in the UK", in Z. Goldman and S. Racoff (eds.), Global Intelligence Oversight: Governing Security in the Twenty-First Century (Oxford University Press, 2016).

[48] Regulation of Investigatory Powers Act 2000, S. 28 (in the case of "directed surveillance" ie covert surveillance in a public place) and S. 29 (in the case of covert human intelligence sources) and Sch. 1.

intrusive surveillance will in any event involve interference with property (for example, to plant and recover covert audio and video devices) and so will fall within the regime for property warrants (issued by the Secretary of State) under the Intelligence Services Act 1994.

The provisions concerning interception of communications and communications **27**
data will be replaced by the Investigatory Powers Act 2016, once it is in force and the account below focuses on those new provisions. A brief explanation is necessary, however, of the context for the changes.

II. The reform of surveillance powers

Prior to the 2016 Act the RIPA provisions drew a distinction between interception **28**
warrants, which identified specific targets for surveillance and were approved individually, and "certificated warrants" for interception of external communications (i. e. where the originator or recipient of the communication was outside the country). The latter, approved by the Foreign Secretary, needed only to specify general categories of information and were then subject to less rigorous controls over the examination of material obtained. Interception of metadata was likewise subject to lighter regulation and could be undertaken by a number of public agencies, after approval of a magistrate.

There was clear evidence before the 2016 reforms that the existing law on surveillance **29**
was being stretched and contradicted in spirit, if not according to the letter, by some of the agencies' practices. RIPA contained some safeguards against use of external communications warrants as a substitute for the targeted interception of internal communications, thus partially addressing one potential concern. What the legislation did not do, however, was to adequately distinguish between metadata and interception of the contents of communication in a way corresponding to current technology. As a result, the weaker controls over gathering metadata allowed for collection of much personal information that a decade earlier would have only been available under the stricter regime governing interception of the content of communications. Nor did the legislation contain any effective safeguards against the transfer of intercepted material to overseas agencies such as the NSA, or deal adequately with controls over material flowing the other way.

The distinction between domestic and external interception was in any event called **30**
into question by the disclosures of Edward Snowden which included allegations that the UK agencies treated communications with overseas based internet platforms (such as yahoo, Google and Facebook) as subject to the external regime. The Intelligence and Security Committee revealed in 2015 that the agencies had sought and ministers had approved "thematic" interception warrants covering defined groups of individuals or networks, rather than identified individuals.[49] Commentators argued that this practice was of dubious legality under the RIPA[50] and the statutory overseer, the Interception of Communications Commissioner, was plainly uncomfortable with it also, although stopping short of labelling it unlawful.[51]

---

[49] Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and Transparent Legal Framework* (March 2015) HC 1075, para 42 ff.

[50] The statutory basis for thematic warrants rests on the definition of a "person" who may be subject to an external warrant which includes "any organisation or any association or combination of persons" [Regulation of Investigatory Powers Act 2000, S. 8(1)]. The Investigatory Powers Act 2016, S. 7(2). aims to remove any doubt by providing that in the context of a single investigation or operation, a warrant can also cover a group of linked persons, or to more than one person or organisation, or set of premises.

[51] T. Hickman, "The Investigatory Powers Bill: What's Hot and What's Not?" U.K. Const. L. Blog (11th Dec 2015) (available at https://ukconstitutionallaw.org/).

31 A series of further admissions and official disclosures followed. The Interception of Communications Commissioner was asked in January 2015 to review the use of a hitherto obscure power contained in the Telecommunications Act 1984 to give ministerial directions to communications providers on grounds of national security.[52] This provision had its roots in the privatisation of telecommunications and pre-dated the widespread availability of mobile phones and internet communications but had nonetheless been used, without reporting its use to Parliament, to allow the agencies to acquire bulk communications data under successive governments.[53] Other techniques that had not previously been acknowledged by the agencies, such as the use of Bulk Personal Datasets and Computer Network Exploitation (computer hacking) were publicly avowed.

32 The UK authorities have attempted to frame the debate about non-targeted data gathering and analysis by careful choice of language, referring to "bulk" powers (in preference to "mass surveillance") to acknowledge the large-scale of the enterprise while nonetheless distinguishing it from universal or indiscriminate intelligence gathering. The account by the ISC of GCHQ's practice stresses, however, that only a small (but unspecified) proportion of internet traffic is collected under these powers, that smaller proportions still are searched by automated means and only very small proportions of these will ever be read by a human analyst.[54] In an effort to demonstrate the need for these powers and to garner bi-partisan support an independent review was commissioned from the Independent Reviewer of Terrorism which endorsed the operational case for the various bulk powers in the IPA 2016.[55]

33 The Investigatory Powers Act 2016 brings the existing powers for the agencies and law enforcement bodies for surveillance of communications and access to communications data together in one place but also significantly extends the powers to cover additional new technologies and allows access to internet connection records. It gives comprehensive statutory underpinning for the first time to a variety of "untargeted" or "bulk surveillance" techniques used by the security and intelligence agencies, in particular, bulk collection and examination, analysis of bulk personal datasets, and also to equipment interference. These are discussed in turn below. Together they reflect the increasing shift in counter-terrorism techniques away from traditional interceptions of communications and towards the collection and analysis of communications data, designed to establish the movement and location of individuals, their habits (including internet browsing), their networks, contacts and travel.

34 Despite the scale of the reforms the government has conceded that the legislation will need some further amendment before being brought into force with regard to retention of communications data, following the decision of the CJEU in *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*.[56] In a consultation document issued in November 2017 the government argued,

[52] The review was published: Report of the Interception of Communications Commissioner, *Review of the Directions given under S. 94 of the Telecommunications Act (1984)*, July 2016, HC 33.

[53] As the Prime Minister acknowledged in a statement to parliament in November 2015: Rt. Hon. Theresa May MP, H.C. Deb., 4 Nov 2015, col. 971.

[54] *Privacy and Security* 31–32.

[55] David Anderson QC, *Report of the Bulk Powers Review*, Cm. 9326 (August 2016).

[56] 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. Tom Watson and Others*, 21 December 2016, CJEU. Following that decision, the Court of Appeal granted a declaration that insofar as the Data Retention and Investigatory Powers Act 2014 (since repealed) permitted use of access to retained data collected for the purpose of preventing, detecting, investigating and prosecuting criminal offences it was not limited to fighting serious crime nor subject to prior review by a court or independent administrative authority: *Watson v. SSHD* [2018]

however, that any changes would affect communications data retention on grounds of investigation of serious crime but not national security, because of the EU's lack of competence in the latter field.[57] Others, however, challenge that contention and further cases are pending to challenge the compatibility of the data retention powers (discussed below) with European law.[58]

III. Targeted interception and examination

Under Part 2, Ch. 1 of the 2016 Act the heads of the three intelligence services and **35**
the Chief of Defence Intelligence may apply to the Secretary of State for an interception warrant.[59] These fall into two main relevant categories: targeted interception warrants and targeted examination warrants. The latter authorise the examination of material relating to a person in Britain that has been collected under a bulk interception warrant.[60] The main changes introduced by the 2016 Act are to place added protections for certain categories of communications onto a statutory footing and to move away from ministerial warrants by introducing judicial approval.

An interception warrant may relate to a particular person or organisation, or a single **36**
set of premises. This re-enacts longstanding practice and earlier legislation. The Act also aims to remove any doubt about the legality of thematic warrants by providing that in the context of a single investigation or operation it can also cover a group of linked persons, or to more than one person or organisation, or set of premises.[61] It is questionable, however, whether it complies with the criteria identified by the Grand Chamber of the European Court of Human Rights in the *Zakharov* case which include the need in order to comply with Art. 8 ECHR to:

> *"clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which authorization is ordered. Such information may be made by names, addresses, telephone numbers or other relevant information"*[62]

Concerning the grounds for a targeted warrant, the Secretary of State may issue an **37**
interception warrant in the interests of national security, for the purpose of preventing or detecting serious crime, in the interests of the economic well-being of the United Kingdom (in circumstances relevant to the interests of national security), or for giving

EWCA Civ 70. The Court of Appeal's judgment does deal with the use of data for national security purposes (see further pending cases below).

[57] Home Office, *Investigatory Powers Act 2016, Consultation on the government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data* (November 2017) 11.

[58] The NGO Liberty has made an application for judicial review (to be heard in February 2018) alleging that the powers under Part IV of the Investigatory Powers Act 2016 for retention of communications data do not comply with the *Watson* judgment. In addition, the Investigatory Powers Tribunal has made a preliminary reference to the CJEU to clarify the application of the *Watson* judgment to Bulk Communications Data retained by the security and intelligence agencies: *Privacy International v. Secretary of State,* UKIP Trib IPT 15 110 CH.

[59] The minister must personally consider the application: Investigatory Powers Act 2016, s. 30.

[60] A targeted examination warrant is required whenever a member of an intelligence service wishes to look at material which relates to a person who is known to be in the British Islands and when he or she believes that it is necessary and proportionate to select the content of that person's communications for examination: Investigatory Powers Act 2016, s. 15(3).

[61] Investigatory Powers Act 2016, S. 7(2). A warrant may also relate to testing or training activities: ibid., S. 7 (3).

[62] *Zahravov v. Russia*, Application 47143/06, para 264, European Court of Human Rights, para 264.

effect to the provisions of a mutual assistance agreement.[63] The minister must personally consider the application and be satisfied that the interception is both necessary[64] and proportionate to the grounds.

38 Special enhanced safeguards apply if the warrant relates to the communications of Members of Parliament. Previously it was thought that that the so-called "Wilson doctrine"[65] prevented interception of communications of MPs and Peers as a matter of constitutional convention. However, the Investigatory Powers Tribunal examined the practice in 2017 and concluded that the doctrine had no strict legal effect.[66] The Tribunal noted, however, that the agencies were bound by codes and guidance (disclosed in the proceedings), which imposed considerable preconditions before parliamentarians' communications could be accessed and that this regime complied with the European Convention on Human Rights. The 2016 Act significantly strengthens the protection for Members of Parliament's communications: in these cases the authorisation of the Prime Minister and a Judicial Commissioner is required.[67]

39 Additional statutory requirements also apply to protect legally privileged material and journalistic material.[68] The introduction of these protections follow a ruling from the Investigatory Powers Tribunal in *Belhadj & Others v the Security Service & Others*[69] that legally privileged material collected under the former legal regime had been unlawfully intercepted in contravention of Art. 8 ECHR, and ordering its destruction.

40 Following the minister's approval a Judicial Commissioner considers whether to approve the warrant (see S. E.III. 1 below for description of judicial oversight), applying judicial review principles to the Secretary of State's conclusions with regard to the necessity and proportionality of the warrant[70] and having particular regard to privacy duties.[71] Where a Judicial Commissioner refuses to approve a warrant written reasons must be given by the Commissioner and these may be reconsidered by the Investigatory Powers Commissioner at the request of the person authorising the warrant. The Investigatory Powers Commissioner's decision is final.[72]

---

[63] Investigatory Powers Act 2016, Ss. 20(2). Sub-s. (4) makes clear that a warrant may only be considered necessary in the interests of the economic well-being of the UK when it relates to the acts or intentions of persons outside the British Islands.

[64] A warrant cannot be considered necessary if its only purpose is gathering evidence for use in legal proceedings, or only on the basis that the information that would be obtained relates to trade union activity in the British Islands [Ss. 20(5) and (6)].

[65] Based on a statement to the House of Commons on 20 June 1966 by the then Prime Minister, Harold Wilson.

[66] *Caroline Lucas MP, Baroness Jones of Moulsecoomb AM, George Galloway vs. the Security Service, SIS, GCHQ* [2017] 1 All ER 283, IPT/14/79/CH IPT/14/80/CH IPT/14/172/CH.

[67] S. 26.

[68] Ss. 27–29.

[69] In *Belhadj & Others v. the Security Service & Others* IPT/13/132-9/H. And see *Privacy International and Greennet & Others v. (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters*, IPT 14/85/CH 14/120-126/CH holding that since changes to the statutory Codes of Practice in 2015 that protection for legally privileged material in relation to Computer Network Exploitation (CNE) by the services had complied with the ECHR.

[70] S. 23.

[71] Set out in S. 2.

[72] Ss. 23(4) and (5).

IV. Untargeted "bulk" powers

Domestic authorisations to obtain communications data are governed by Part 3 of the 2016 Act. This provides for "bulk acquisition"[73] i. e. an instruction to a telecommunications operator to retain communications data[74] and disclose it to the intelligence services[75] (or so-called metadata) and for the retention and examination of bulk personal datasets.[76] **41**

Before exercising one of the "bulk" powers, the services must obtain a warrant authorised by the Secretary of State and approved by a Judicial Commissioner. The warrants must specify the operational purposes for which any communications data obtained may be selected for examination. The operational purposes provided for in the Act are: national security; or national security and the purpose of preventing or detecting serious crime; or national security and in the interests of the economic well-being of the United Kingdom.[77] The 'operational purposes' approved by the Secretary of State for bulk interception must, however, be specified in greater detail than the general description 'national security', and moreover are required to be shown at 3-monthly intervals to the Intelligence and Security Committee.[78] **42**

When bulk acquisition is used domestically the intelligence services may only collect communication data rather than the content of the communications.[79] This could nonetheless include the location of mobile and fixed line phones from which calls are made or received, and the location of computers used to access the internet, the identity of a subscriber to a telephone service or a detailed telephone bill, websites visited from a device, email contacts, map searches, GPS location and information about devices connected to a Wifi network. Such data can, for example, be used by the agencies to identify members of a terrorist network in contact with a particular email address.[80] **43**

Techniques used for foreign surveillance gathering by contrast are more intrusive and allow for the collection and access of content of communications rather than only metadata.[81] The Act allows bulk collection through "interception of overseas-related communications"[82] (i. e. sent or received by a person outside Britain) and "obtaining secondary data from such communications".[83] One method used by the intelligence services is to tap undersea fibre optic cables landing in the United Kingdom in order to intercept their traffic. Indeed in 2008 the European Court of Human Rights found that a programme of mass interception of "external" communications passing between the **44**

[73] Privacy International challenged the bulk acquisition powers under S. 94 of the Telecommunications Act 1984 before the Investigatory Powers Tribunal. The IPT ruled that until 4 November 2015 when stricter safeguards were introduced, the intelligence services were violating the right to private life (Article 8 of the ECHR): *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIP Trib 15_110-CH, 17 October 2016.

[74] Under the terms of the Act communications data refers to the "who", "when", "where" and "how" of a communication, but not its content.: see Ss. 261 and 262.

[75] Investigatory Powers Act 2016, Ss 158–175.

[76] Investigatory Powers Act 2016, Ss. 199–226.

[77] Investigatory Powers Act 2016, S. 138 (bulk interception); S. 158 (bulk acquisition); S. 178 (bulk equipment interference); Ss. 204 and 205 (bulk personal datasets).

[78] Investigatory Powers Act 2016, S. 142 (bulk interception); S. 161 (bulk acquisition); S. 183 (bulk equipment interference); S. 212 (bulk personal datasets).

[79] Investigatory Powers Act 2016, S. 158(6).

[80] Anderson, *A Question of Trust* (2016), p. 159.

[81] Investigatory Powers Act 2016, Part 6 Ch. 1.

[82] Investigatory Powers Act 2016, S. 136 (2)(a).

[83] Investigatory Powers Act 2016, S. 136 (2)(b).

Republic of Ireland and the UK operated by the Ministry of Defence under warrant between 1990 and 1997 violated Article 8, because the statutory basis was insufficiently clear and detailed.[84] The provisions governing ministerial approval of "operational purposes" described above go some way to meet the criticism that the 2016 Act permits "mass surveillance". However, the language used to describe these would still allow a high degree of generality in the authorization of bulk powers and a number of the controls governing how analysts can query databases of collected data remain in the form of internal procedures, rather than legal requirements.

V. Bulk personal datasets

45 Bulk personal datasets are large datasets containing information about a large number of individuals (such as passport holders, driving licence records, voters on the electoral register) that are incorporated into "analytical systems". The majority of the individuals to whom this data relate will not be of any interest to the intelligence services but they will examine the data relating to the minority who are of intelligence interest. The data may be acquired by overt or covert means, and include data about biographical details, commercial and financial activities, communications and travel.

46 Although it is hardly surprising that services access and link personal data in this way, the existence their use of bulk personal datasets was only confirmed for the first time in 2015.[85] In its Privacy International decision the Investigatory Powers Tribunal found that the intelligence services had violated the right to private life until 12 March 2015 when stricter safeguards were introduced.[86] Whereas previously the agencies claim of authority to access and use Bulk Personal Datasets rested only on their general statutory competences, the 2016 Act now gives an express statutory basis for their retention and use.

47 The 2016 Act defines them as sets of "information that includes personal data relating to a number of individuals"[87] where "the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions".[88] It provides that BPDs may not be retained or examined by an intelligence agency unless authorised by warrant.[89] Warrants are of two kinds: Class or Specific BPDs.[90]

48 An intelligence agency is prevented from using a class BPD warrant to access a dataset that consists of health records or if a substantial proportion of the dataset consists of sensitive personal data.[91] For this purpose, the definition of "sensitive personal data" corresponds to that for data protection purposes i. e. a person's racial or ethnic origins, political or religious beliefs, trade union membership, health, sexual life, and criminal record.[92] A restriction also prohibits retention or examination of a BPD in reliance on a class BPD warrant if the head of the intelligence service considers that the

[84] *Liberty and Others v. United Kingdom,* Applicationno. 58243/00, E Ct HR, 1 July 2008.
[85] Intelligence and Security Committee of Parliament (2015), Ch. 7.
[86] Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 17 October 2016.
[87] Investigatory Powers Act 2016, S. 199 (1)(a).
[88] Investigatory Powers Act 2016, S. 199 (1)(b).
[89] Investigatory Powers Act 2016, S. 200.
[90] Investigatory Powers Act 2016, Ss. 204 and 205, respectively.
[91] S. 202(1). Nor may an intelligence service retain, or retain and examine, a BPD in reliance on a class BPD warrant if the head of the intelligence service considers [the BPD consists of, or includes such personal data (s. 202(2)].
[92] Data Protection Act 1998, S. 2(a)-(f).

nature of the BPD raises novel or contentious issues which ought to be considered by the Secretary of State and a Judicial Commissioner.

VI. Equipment interference

Part V of the 2016 Act gives for the first time explicit powers for interference by the **49**
agencies with equipment (typically, computers and mobile devices). Hitherto the agencies have relied on less specific powers to interfere with property, which in public accounts had been associated with covert entry to premises in order to search, place or recover surveillance devices. In its *Greenmet* decision the Investigatory Powers Tribunal found that existing powers for property interference warrants (under S. 5 of the Intelligence Services Act 1994 and with reference the statutory Codes of Practice) could in principle be used to allow GCHQ to carry out Computer Network Exploitation (CNE) and gave guidance over how specific a warrant would have to be in order to be lawful both at domestic law and so as to comply with Articles 8 and 10 of the ECHR.[93] The Tribunal reached no conclusion whether s. 7 of the Intelligence Services Act 1994 (which allows ministerial authorization of otherwise unlawful extra-territorial acts by the services) could lawfully authorize CNE outside the British Islands, because of its uncertainty over whether the Convention would apply, at least in relation to a hypothetical case. The 2016 Act covers the topic explicitly and provides for equipment interference warrants to be issued by the Secretary of State[94] and to be approved by a Judicial Commissioner.[95] If the Commissioner refuses to approve the warrant the agency may ask the Investigatory Powers Commissioner to review the decision.[96]

Bulk equipment interference[97] is only permitted if outside Britain.[98] It covers 'hacking **50**
or the implantation of software into endpoint devices or network infrastructure to retrieve intelligence, but [they] may also include, for example, copying data directly from a computer'.[99] Presumably also, though not explicitly acknowledged, the interference could take the form of implanting malware in a cyber-attack. It is alleged, for example, that GCHQ participated, together with US and Israeli agencies, in the development of the so-called Olympic Games virus to disable critical infrastructure in advance of a potential Israeli attack on the Iranian nuclear programme.[100]

[93] *Privacy International and Greenmet & Others v. (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters*, IPT 14/85/CH 14/120-126/CH.

[94] Investigatory Powers Act 2016,S. 102. A warrant can only be issued if it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or in the interests of the economic wellbeing of the United Kingdom (so far as those interests are also relevant to the interests of national security) (s.102(5)) and proportionate to the intended outcome.

[95] Investigatory Powers Act 2016, S. 108.

[96] Investigatory Powers Act 2016, S. 108(5).

[97] Investigatory Powers Act 2016, Part 7.

[98] Investigatory Powers Act 2016, s 176(1)(c). Prior to the entry into force of the Investigatory Powers Act 2016, bulk powers interference had never been used in the United Kingdom. Anderson, D. (2016), 184.

[99] Anderson, *A Question of Trust,* (2016), 34.

[100] 'Zero Day: Nuclear Cyber Sabotage', BBC television, 16 Jan 2017.

VII. The judicial approval process

51 The 'double-lock,' approval process introduced in the 2016 Act requires that warrants or notices for both targeted surveillance and bulk powers be authorised by the Secretary of State[101] and subsequently approved by the Judicial Commissioner.[102] Judicial Commissioners must hold or must have held a high judicial office.[103] The 'double-lock,' is a major change and replaces a procedure dating back to the sixteenth century under which ministers alone were responsible for issuing warrants for interception.

52 This change follows longstanding criticism that the system of ministerial warrants lacked the independence and rigour of a judicial process in protecting human rights and was out of line with international practice. These considerations, together with the pragmatic argument that a judicial process was more likely to persuade the major US communications providers to cooperate with requests from the UK agencies,[104] led to proposals to put final approval in the hands of a Judicial Commissioner. The Intelligence and Security Committee had suggested that ministers should continue to issue warrants rather than judges because they were better able to judge the wider public interest, as well as the diplomatic and political context, while being politically responsible for decisions to authorize surveillance.[105] As the Independent Reviewer pointed out, however, in view of the secrecy surrounding surveillance, responsibility was notional rather than a realistic prospect of being called to account. He recommended a system of judicial warrants, with a variation of a mixed system in the case of national security warrants relating defence and foreign affairs. The latter system would retain the advantages of ministerial approval but place consideration of more distinctly legal questions into the hands of a Judicial Commissioner.[106] It is a variation on this division of labour, applying it more widely, that has been implemented in the 'dual lock' provisions.

53 Under the process the Commissioner is required to review whether the warrant or notice is necessary and whether the measures applied for are proportionate.[107] Warrants are valid for six months,[108] and retention notices can require the retention of data for 12 months.[109] In urgent cases a warrant can be issued for targeted interception and equipment interference and as well as for bulk interception and bulk datasets without the prior approval of the Judicial Commissioner.[110] In these cases, however, the Commissioner must be notified and can decide whether they approve the warrant or not within three working days after the date of issue. In cases of refusal to approve a

[101] Investigatory Powers Act, s. 19 for interception and examination, s. 87 for retention of communications data, s. 102 for equipment interference.

[102] Investigatory Powers Act, s. 23 for interception and examination; and S. 87 (1) (b) for retention notices, S. 102 (1) (d).

[103] Investigatory Powers Act, S. 227 (2).

[104] *A Question of Trust* 207.

[105] *Privacy and Security* 119.

[106] *A Question of Trust*, 274.

[107] Investigatory Powers Act, S. 23 (1) for interception and examination, S. 89 (1) for retention, S. 108 (1) for equipment interference.

[108] Investigatory Powers Act, S. 32 (2) (b) for interception and examination, S. 116 (2) (b) for equipment interference.

[109] Investigatory Powers Act, S. 87 (3).

[110] Investigatory Powers Act 2016, Ss. 24 and 109 for targeted interception and examination, and equipment interference warrants respectively. S. 180 for bulk equipment interference, s. 209 for bulk personal datasets.

warrant, then the implementing authority must, "so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible".[111] The Commissioner may also decide whether to request the destruction of any material collected or may impose conditions on its use or retention.[112]

E. Accountability of the agencies

I. Ministerial responsibility and control

Ministerial responsibility for the Security Service is through the Home Secretary, although operational control is in the hands of the Director-General. SIS and GCHQ both come under the authority of the Secretary of State for Foreign and Commonwealth Affairs. Operational control is in the hands of the Chief and Director, respectively, who are appointed by the minister.[113] Each agency head is required to give an annual report to the Prime Minister and the Secretary of State. **54**

It would be wrong, however, to equate the position of the agencies with conventional government departments of state, responsible to a Secretary of State. There is a marked departure from the British constitutional position by which ministers are legally responsible and officials are anonymous and, legally-speaking, invisible. Statutory provisions give the heads of the agencies a right of direct access to the Prime Minister[114] who, despite the services' departmental associations, has traditionally assumed overall control and acted as the government mouthpiece on intelligence matters.[115] Moreover, unlike normal civil service heads of department the Director-General of the Security Service, the Chief of the SIS and the Director of GCHQ are named in law as having day to day responsibility. The reason is undoubtedly to provide a safeguard of the services' neutrality in party political terms. Indeed, political neutrality is explicitly addressed by provisions that require the heads of all three agencies to ensure that the services do not take any steps to further the interests of any UK political party.[116] **55**

Furthermore, some of the services' actions require explicit ministerial approval by the responsible Secretary of State. Unlike many other countries in which judicial authorisation is required, in the UK the tradition has been for telephone tapping or mail opening (which may also be undertaken by the police) to be approved by the Secretary of State under warrant.[117] This process will, however, be modified by the addition of a process of judicial confirmation once the 'dual lock' system under the Investigatory Powers Act 2016 comes into force. Another instance where ministers are given specific powers concerning individuals is the field of detention of terrorist suspects and the deportation of foreign nationals on grounds of national security.[118] Diligent ministers will clearly require convincing and detailed supporting evidence from the agencies before they approve such actions. In the current context of use of counter-terrorist powers, for **56**

[111] Investigatory Powers Act 2016, Ss. 25 (2); 110 (2); 181 (2); 210 (2) respectively.
[112] Investigatory Powers Act 2016, S. 25 (3).
[113] Intelligence Services Act, Ss. 2 and 4.
[114] Security Service Act 1989, S. 2(4) and Intelligence Services Act 1994, Ss. 2(4) and 4(4).
[115] See also: R. Aldrich and R Cormac, *The Black Door: Spies, Secret Intelligence and British Prime Ministers* (Harper Collins, 2016).
[116] Security Service Act 1989, S. 2; Intelligence Services Act 1994 1994, Ss. 2 and 4.
[117] Regulation of Investigatory Powers Act 2000, Part 1. In practice, the Home Secretary, Foreign Secretary, Northern Ireland Secretary, the Secretary of State for Defence, and the Second Minister in Scotland.
[118] Under the Anti-Terrorism Crime and Security Act 2001 and the Immigration Act 1971.

example, a close and continuous dialogue between the Home Secretary, her officials and the Security Service is inevitable. Similarly the implications of the actions of SIS and GCHQ for diplomatic and foreign relations create an imperative for consultation with the Foreign Secretary. In some instances this is buttressed by legal requirements also: when immunity is required from legal liability under UK law for actions abroad (i. e. for offences over which the UK courts exercise extra-territorial jurisdiction) the Foreign Secretary may give authorisation under section 7 of the (Intelligence Services Act 1994.

57 The budgets of the agencies are set by ministers through the Single Intelligence Account (SIA) as part of the government-wide periodic Spending Review mechanism. Individual agency budgets are not published annually because the information is deemed sensitive. The Prime Minister' s National Security Adviser is the Principal Accounting Officer for the SIA. Defence Intelligence and the central intelligence machinery are funded separately through the Ministry of Defence and the Cabinet Office respectively. JTAC is funded by the various departments and agencies contributing staff with additional costs covered through the SIA.

II. Parliamentary oversight[119]

58 The Intelligence and Security Committee ('ISC'), was established under the Intelligence Services Act 1994 to examine all three security and intelligence services. The Justice and Security Act 2013 made some (mostly minor) changes to the ISC's composition, reporting and remit and is the current legislation.

59 Under the Justice and Security Act 2013 the ISC was re-designated as the Intelligence and Security Committee *of Parliament* (emphasis added), with a remit to examine the expenditure, policy and administration of all three security and intelligence agencies.[120] This is a subtle difference which the government argued would make the Committee 'demonstrably accountable to Parliament'.[121] The ISC can oversee other parts of the intelligence community under a memorandum of understanding agreed with the Prime Minister.[122] It has restricted powers to examine operational matters where the agencies volunteer information or (in the case historic operations) where requested by the Prime Minister and both the committee and the Prime Minister consider it to be of significant national interest.[123]

60 Unlike a select committee the ISC is governed by legislation, rather than the standing orders of Parliament. The legislation governs the appointment of its members, the procedure it adopts, its powers over witnesses and hearings, and the publication of its reports. It comprises nine Parliamentarians from both Houses, appointed by the respective Houses (to be eligible however they must be nominated by the Prime Minister after consultation with the Leader of the Opposition).[124] Parliament can veto

[119] On parliamentary handling of intelligence more generally, see: I. Leigh and L. Lustgarten, *In From the Cold*, Ch. 16; A.Horne and C. Walker, 'Parliament and National Security' in Horne, A. and Le Sueur, A. (eds.), *Parliament: Legislation and Accountability* (Hart, Oxford, 2016); V. Fikfak and H.Hooper, *Parliament's Secret War* (Hart, Oxford 2018).

[120] Justice and Security Act 2013, S. 2(1). The agencies' expenditure is audited under arrangements with the National Audit Office. The Chair of the House of Commons Public Accounts Committee is also shown the relevant details.

[121] Ministry of Justice, *Justice and Security Green Paper* (2011), Cm 8194: para 3.20; and para 3.25–3.32, discussing incidental changes to the appointment of the members and Chair of the ISC and to the arrangements for its accommodation, staffing and budget.

[122] Justice and Security Act 2013, Ss. 2(2) and (5). On this basis it also examines Defence Intelligence.

[123] Justice and Security Act 2013, S. 3.

[124] Justice and Security Act 2013, S. 1 (3) and (4)(a).

the Prime Minister's nominees to the Committee but does not have a free choice of nominees. Current Ministers of the Crown are legally debarred from being members of the committee.[125]

61 Certain additional practices have supplemented the statutory provisions. The composition has usually been eight members of the House of Commons and one member of the House of Lords. Members have frequently included past holders of ministerial office with experience of responsibility for security and intelligence (including past Foreign, Defence and Home Secretaries) and retired senior civil servants. In the past Prime Ministers have made conspicuous use of the patronage of appointing the chair of the ISC: the chair has been held by a succession of ex-ministers from the party of government. Arguably, confidence in the independence of the committee has been weakened by the failure to rotate the chairmanship with the Opposition.[126] Under the changes introduced in 2013 the Chair is chosen by the Committee itself, rather than by the Prime Minister.[127] The ISC now also reports direct to Parliament but must send its reports beforehand to the Prime Minister and exclude matters that the Prime Minister considers would be prejudicial to the agencies.[128] This is a minor symbolic change to the previous practice whereby the report was to the Prime Minster who then laid it before Parliament. Despite the changes the ISC falls short of being under full control of Parliament in the same way as a select committee.[129]

62 Although the ISC has power to send for persons and papers, in other respects its information-gathering powers are limited. The agency heads may refuse to disclose 'sensitive information'[130] ie information that might lead to the identification of sources, other forms of assistance given to the agencies, or operational methods; information concerning past, present, or future specific operations; or, information provided by a foreign government which does not consent to its disclosure is included. Within these categories refusal is *discretionary*.

63 In practice the ISC works by consensus, perhaps because it meets almost exclusively in private. The published reports do not record formal disagreement or voting among members of the Committee and nor have there been any published minority reports. Nevertheless in the past the Committee has arguably been hampered in its work by being too closely associated with the agencies- particularly when tackling controversial topics such as intelligence before the Iraq war, the 7 July 2005 bombings in London[131] and allegations of complicity in torture.[132] As a consequence of the inability of the ISC to produce definitive reports that allayed public concern and mistrust surrounding these topics there have been several ad hoc inquiries into topics that the ISC has already investigated, for example the Butler review, the special inquest into the 7/7 bombings.[133] The perception that the oversight regime was failing to provide public assurance that

[125] Justice and Security Act 2013, S. (4)(b).

[126] It appeared that a convention of this kind (or of rotating the chair between parties) might emerge when the Labour Prime Minister Tony Blair retained Tom King (a former Conservative minister) as Chair of the ISC following the 1997 election. However, on King's departure there followed a succession of appointments of ex-ministers from the ruling party.

[127] Justice and Security Act 2013, s. 1(6).

[128] Justice and Security Act 2013, s. 3.

[129] As advocated by the Joint Committee on Human Rights, *Allegations of UK Complicity in Torture, 23rd Report for 2008–9*, HL 152/HC 230 (2009). For earlier similar proposals see Home Affairs Select Committee, *Accountability of the Security Service,* HC (1998–99), p. 291.

[130] Justice and Security Act 2013, Sched. 1.

[131] Intelligence and Security Committee 2006. *Report into the London Terrorist Attacks of 7 July 2005*, Cm 6785; Intelligence and Security Committee 2007, *Rendition*, Cm. 7171 (July 2007).

[132] Joint Committee on Human Rights 2009, *23rd Report for 2008–9*, HL 152/HC 230.

[133] *Report of the Official Account of the Bombings in London on 7th July 2005,* H.C. 1087 (2005–6).

the agencies were acting efficiently and with propriety was undoubtedly a major contributing factor to the 2013 reform of the Committee's status and powers. Nonetheless, a MORI survey in 2014 found that 48 % of these survey were "not at all confident" or "not very confident" in the system of oversight in holding the agencies to account, compared to 40 % who were "fairly confident" or "very confident".[134]

64 The ISC has now been in operation for over more than two decades under some 7 different chairs and consequently it is difficult to generalise about its effectiveness. Commentators have given its work mixed reviews.[135] Most accept that it has built up a relationship of trust with the agencies (with only exceptional leaks of confidential material) and that this has enabled it to investigate matters above and beyond those in its remit, including some with operational aspects. It has been seen as fulfilling an educative role in bridging the secret and political worlds.[136] Others, however, have seen the relationship with the agencies as too close, sometimes bordering on advocacy,[137] or on occasion naïve, have criticised it for lack of ambition[138] and inattention to human rights concerns,[139] and have contrasted the quality of its investigations with those other inquiries.[140]

III. Judicial oversight[141]

1.The Commissioners

65 The agencies are also overseen by judicial Commissioners, who were appointed initially under the 1989 and 1994 Acts but currently work within the Regulation of Investigatory Powers Act 2000. These procedures were initially introduced in a (successful) attempt to ward off a finding that the previous regime violated the European Convention on Human

[134] Ibid., 39.

[135] P. Gill, "Evaluating Intelligence Oversight Committees: the case of the UK Intelligence Security Committee and the 'War on Terror' "Intelligence and National Security, 22(1) 14–37 (2207); I. Leigh, "Parliamentary Oversight of Intelligence in the UK: A Critical Evaluation" in H. Born and M. Caparini (eds.) Democratic Control of Intelligence Services: Containing Rogue Elephants (Aldershot: Ashgate 2007); A. Glees, J. Morrison and P. Davies, *The Open Side of Secrecy: Britain's Intelligence and Security Committee* (London: Social Affairs Unit, 2006); M. Pythian, 'A Very British Institution': The Intelligence and Security Committee and Intelligence Accountability in the United Kingdom', in Loch K. Johnson (ed.), *Oxford Handbook of National Security Intelligence* (New York, Oxford University Press, 2010), 699–718; M. Pythian, "The British Experience with Intelligence Accountability: The First Twenty Years", in Loch K. Johnson (ed.) *Essentials of Strategic Intelligence* (Santa Barbara, CA, Praeger Security International, 2015), 447–69; H.Bochel, A. Defty, J. Kirkpatrick "New mechanisms of independent accountability: select committees and Parliamentary scrutiny of the intelligence services" Parliamentary Affairs, 68 (2) 314–331 (2015).

[136] A. Defty, "*Educating parliamentarians about intelligence: the role of the British Intelligence and Security Committee" (2008) 61(4)* Parliamentary Affairs 621–641.

[137] See, for example, its criticism of US-based internet companies for their lack of cooperation with the agencies: Intelligence and Security Committee, *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, 139–151.

[138] P. Gill, "The ISC and the Challenge of International Security Networks", Review of International Studies 35 (2009) p. 932.

[139] I. Leigh, "Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade After 9/11" (2012) 27 (5) Intelligence and National Security 721–737.

[140] R. Aldrich, "Whitehall and the Iraq War: the UK's Four Intelligence Enquiries" Irish Studies in International Affairs, 16 (2005), 73–88.

[141] In addition to the methods described here judges are from time to time to called upon by the government to conduct ad hoc inquiries into matters of public concern involving intelligence: I. Leigh,"The Role of Judges" in S. Farson and M.Pythian (eds), *Commissions of Inquiry and National Security: Comparative Approaches* (Praeger, 2010), ch. 16.

Rights.[142] The legislation is in the process of being supeceded by the Investigatory Powers Act 2016, the oversight arrangements of which are being introduced in phases, from spring 2018. Formerly the Intelligence Services Commissioner was responsible for reviewing and reporting upon the issue and authorization, by the relevant minister, of warrants for operations by the Agencies.[143] The Interception Commissioner (established under S. 57 of the Regulation of Investigatory Powers Act 2000) reviewed the issue and authorization of warrants to intercept mail and telecommunications by the intelligence and security Agencies and law enforcement organizations.

66 The Investigatory Powers Act 2016 makes significant changes to this scheme by bringing together in a single and more powerful judicial Commissioner's office the various oversight Commissioners established under earlier legislation (so abolishing the offices of the Interception Commissioner and Intelligence Services Commissioner). The new Investigatory Powers Commissioner ('IPC') must hold or must have held a high judicial office[144] but the Commissioner's role is distinct from that of the Judicial Commissioners under the Act.[145] The role of the office is to keep under review the majority of the targeted and bulk surveillance powers available to the intelligence services,[146] especially with regard to the operation of safeguards to protect privacy.[147] The security and intelligence services are required to disclose or provide all the necessary documents and information for the purposes of the IPC's functions[148] and to give any assistance the IPC requires in accessing apparatus, systems or other facilities of the intelligence services when exercising oversight functions.[149] The IPC is required to report annually[150] or at any time requested by the Prime Minister[151] or where the Commissioner considers it appropriate.[152] The Prime Minister is obliged to publish the Commissioner's annual reports and to lay a copy of it before Parliament, together with a statement whether any matter has been excluded.[153] In excluding material on the permitted grounds[154] the Prime Minster is required to consult with the Commissioner.[155]

67 The creation of the IPC combats the fragmentation of oversight in which multiple actors had responsibility for examining a narrow function of the agencies or a specific type of review. Instead the IPC brings these functions together, with the possibility of benefiting from joining up or cross-fertilisation from these different oversight activities. The resources available to the new office (the IPC has 50 staff), also underline the trend

[142] The 1989 Act was treated as sufficient reason by the Convention organs to take no further action in cases brought (by Patricia Hewitt and Harriet Harman and dating to their involvement with the National Council for Civil Liberties) involving alleged surveillance and recording of personal details by the Security Service: Council of Europe Resolution DH(90) 36 of 13 December 1990. Later decisions have confirmed that system of Commissioners and tribunal has been found to satisfy Art. 6, 8 and 13 of the European Convention on Human Rights: *Case of Kennedy v UK*, App. *no*. 26839/05, European Court of Human Rights, 18 May 2010. See also: *Esbester v. UK*, App. no. 18601/91, 2 April 1993; *G, H, and I v. UK* (1993), 15 EHRR CD 4.

[143] Regulation of Investigatory Powers Act 2000, S. 59.

[144] Investigatory Powers Act 2016, S. 227 (2).

[145] Investigatory Powers Act 2016, S. 229 (4).

[146] Investigatory Powers Act 2016, S. 229 (1).

[147] Investigatory Powers Act 2016, S. 229 (5).

[148] Investigatory Powers Act 2016, S. 235 (2).

[149] Investigatory Powers Act 2016, S. 235 (3) and (4).

[150] Investigatory Powers Act 2016, S. 234 (1).

[151] Investigatory Powers Act 2016, S. 234 (3).

[152] Investigatory Powers Act 2016, S. 234 (4).

[153] Investigatory Powers Act 2016, S. 234 (6).

[154] Investigatory Powers Act 2016, S. 234 (7).

[155] Investigatory Powers Act 2016, S. 234 (7).

towards expert review. Following the recommendation of the Bulk Powers Review there is a new technical advisory panel to assist the Commissioner's office.[156] Moreover, instead of being a responsive institution that either reports or is tasked the IPC has own-initiative powers to conduct thematic reviews of capabilities and to investigate serious errors.[157]

2. Investigatory Powers Tribunal

68 A specialist body the Investigatory Powers Tribunal (the 'IPT'), has been established to investigate public complaints against the agencies or allegations of illegal interception by them.[158] Members of the tribunal must hold or have held high judicial office or be qualified lawyers of at least ten years' standing. Any person may bring a claim and the IPT must determine all claims brought before it, except those it considers to be vexatious or frivolous.[159] The IPT is specified as the only appropriate forum for proceedings against any of the intelligence services concerning alleged incompatibility with European Convention rights and for complaints by persons who allege to have been subject to the investigatory powers of the Regulation of Investigatory Powers Act.[160] It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. It is required to follow the principles applicable by a court on an application for judicial review[161] and can require anyone involved in the authorisation and execution of an interception warrant to disclose or provide documents and information[162] and all such assistance as it thinks fit from a relevant Commissioner.[163] At the conclusion of proceedings the IPT is required to give a simple statement either that they have found in favour of the complainant (i. e. that there has been unlawful action against him or her) or that ' no determination has been made in his favour'.[164] This safeguards information about the agencies so that proceedings cannot be used to discover whether or not a person is lawfully under surveillance. In the event of a successful claim the IPT is also required to submit a report to the Prime Minister.[165] The IPT has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling interception warrants and requiring the destruction of any records so obtained.[166] There is currently no appeal,[167] although once in force the Investigatory Powers Act 2016 will introduce an appeal on a point of law to the Court of Appeal.[168] The procedure before the IPT has been found to be compatible with Article 6 of the ECHR.[169]

---

[156] Investigatory Powers Act 2016, Ss.246 and 247.

[157] See below.

[158] Regulation of Investigatory Powers Act 2000, S. 65.

[159] Regulation of Investigatory Powers Act 2000, Ss. 67(1), (4) and (5).

[160] Regulation of Investigatory Powers Act 2000, S. 65(2). In *R (A) v Director of Establishments of the Security Service* [2009] UKSC 12; [2010] 2 AC 1 the UK Supreme Court confirmed that this provision prevented other courts from hearing claims under S. 7 of the Human Rights Act 1998 against any of the intelligence services.

[161] Regulation of Investigatory Powers Act 2000, Ss. 67(2) and 67(3)(c).

[162] Regulation of Investigatory Powers Act 2000, Ss. 68(6) and (7).

[163] Regulation of Investigatory Powers Act 2000, S. 68(2).

[164] Regulation of Investigatory Powers Act 2000, S. 68(4).

[165] Regulation of Investigatory Powers Act 2000, S. 68(5).

[166] Regulation of Investigatory Powers Act 2000, S. 67(7).

[167] Regulation of Investigatory Powers Act, S. 67(8). This provision has also been held by the Court of Appeal to preclude judicial review of the Tribunal's decisions: *R (Privacy International) v. Investigatory Powers Tribunal* [2017] EWCA Civ 1868.

[168] Investigatory Powers Act 2016, S. 242.

[169] *Kennedy v UK* (2011) 52 EHRR 4.

Despite the restrictions built into the statutory scheme, in a series of careful judgments (mostly arising from the Snowden allegations) the IPT has succeeded in crafting within its limited powers a procedure for dealing with serious allegations notwithstanding the agencies' policy to neither confirm nor deny them. This procedure allows for the relevant legal arguments to be determined on the basis of "hypothetical facts". Consequently, the IPT is able to make a binding pronouncement of legal principle even if it is unrealistic for the claimant to be able to discharge the burden of proof. This procedure was adopted by the IPT in dealing with the claim brought by Privacy International and other NGOs that the alleged involvement of the GCHQ in the PRISM and TEMPORA programmes was unlawful.[170] The Investigatory Powers Tribunal found that GCHQ involvement in the TEMPORA programme, alleged by Snowden, lacked a basis in domestic law. It held that the searching by GCHQ of bulk data collected by the NSA had been in violation of Art. 8 of the European Convention on Human Rights but that this defect had been cured for the future by the disclosure (during the proceedings in question) of previously secret internal guidance.[171] A similar approach was followed by the IPT in its *Greenmet* decision, holding that since changes to the statutory Codes of Practice in 2015 protection for legally privileged material in relation to Computer Network Exploitation (CNE) by the services had complied with the ECHR.[172] It remains to be seen whether this approach to the foreseeability and accessibility tests under Art. 8 (2), which essentially allows the agencies to benefit from previously secret internal procedures disclosed only at the courtroom door, will be accepted by the Strasbourg court.[173] Nonetheless the IPT, which was previously a rather under-rated body, has earned a measure of respect for these and other decisions which show careful analysis and some robustness in dealing with claims from the agencies. A notable instance was its ruling in in *Belhadj & Others v the Security Service & Others*[174] that legally privileged material had been unlawfully intercepted in contravention of Article 8 ECHR and ordering its destruction. In the words of the Independent Reviewer of Terrorism Legislation, the IPT has 'stepped out of the shadows'.[175] **69**

The Tribunal may be further strengthened by changes in the 2016 Act connecting the IPT's complaints-based jurisdiction and the IPC's audit role. The existing duty of the Commissioner to assist the IPT has been supplemented by a duty to give the Tribunal the Commissioner's opinion on relevant matters, which will allow the Commissioner's expertise to assist the Tribunal.[176] There is also a duty to inform a person affected by a serious error (i. e. one that has caused them significant prejudice or harm) in matters under the Commissioner's review where the Commissioner determines that this is in the public interest.[177] The person concerned must also be informed of their right to apply to the IPT and given sufficient details to enable them to do so. This is should make it substantially easier to bring a successful complaint to the IPT against the security and intelligence agencies in appropriate cases, although much will turn on the **70**

[170] Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77 –H.

[171] *Liberty and others v. The Secretary of State for Foreign and Commonwealth Affairs and others*, no. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIP Trib 13_77 –H at 153–154.

[172] *Privacy International and Greenmet & Others v. (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters*, IPT 14/85/CH 14/120-126/CH.

[173] Similar questions are pending before the European Court of Human Rights: *Big Brother Watch and Others v. the United Kingdom*,no. 58170/13, 7 January 2014.

[174] In *Belhadj & Others v the Security Service & Others* IPT/13/132-9/H.

[175] *A Question of Trust*, para. 6.107.

[176] Investigatory Powers Act 2016, S. 232.

[177] Investigatory Powers Act 2016, S. 231.

IPC's assessment of when it is in the public interest to inform the individual concerned. In principle the hand of the IPT in reaching its own assessments (and consequently public confidence in the process) should also be strengthened by the enhanced power to draw on the expertise of the IPC. At the same time the IPT has introduced the procedural innovation of appointing counsel to the tribunal to assist it in challenging material from the security and intelligence agencies.[178]

F. Intelligence and the courts

I. The courts and deference to national security

71 The courts themselves have long recognized that decisions based on national security are for the government and that judges have neither the necessary information nor the competence to assess these questions. Famously in the 1984 GCHQ case (concerning the legality of the government's ban on trade union membership) Lord Diplock explained:

> *"National security is the responsibility of the executive government; what action is needed to protect those interests is ….a matter upon which those upon whom the responsibility rests, and not the courts of justice, must have the last word. It is par excellence a non-justiciable question. The judicial process is totally inept to deal with the sort of problems which it involves."*[179]

72 This approach has been followed both in wartime and in peacetime in a line of judicial decisions now dating back a century, to the First World War.[180] Perhaps the high point of judicial deference to governmental claims of national security in modern times came in Lord Denning's 1977 judgment in the case of an unsuccessful challenge brought by the American journalist Mark Hosenball to his deportation on national security grounds following magazine article that he had written about GCHQ. His Lordship stated that the rules of natural justice (which would have normally required disclosure of material to allow Hosenball to challenge the decision) had to be 'modified' when security was at stake:

> *"There is a conflict here between the interests of national security on the one hand and the freedom of the individual on the other. The balance between these two is not for a court of law. It is for the Home Secretary."*[181]

73 Following 9/11 a more sceptical attitude prevails. For example, where the government advances arguments that are contradictory or has chosen measures that interfere disproportionately with individual rights then the courts do now intervene- as the House of Lords' landmark decision in the *Bellmarsh* detainees' case shows. The House of Lords ruled that the provisions in Part IV of the Anti-Terrorism Crime and Security Act 2001 dealing with detention without trial of non-nationals were incompatible with the European Convention, despite a purported derogation from Article 5 (the right to liberty).[182] A majority of the court found that because of the potentially devastating

[178] As recommended by the Independent Surveillance Review, *A Democratic Licence to Operate* 113.
[179] *Council of Civil Service Unions v. Minister for the Civil Service* [1985] A.C. 374, 412.
[180] L. Lustgarten and I. Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford, 1994) ch. 12.
[181] *R v Secretary of State for the Home Department ex parte Hosenball* [1977] 3 All E.R. 452, 461.
[182] *A (FC) and Others (FC) v Secretary of State for the Home Department*, [2004] UKHL 56; [2005] 2 WLR 87.

consequences of an attack the government was not wrong to invoke the derogation, but that the powers that it claimed on this basis were disproportionate. Some of the judicial comments are worth noting for comparison to earlier statements from the bench. Lord Scott, while deferring to the Secretary of State on whether there was a public emergency within Article 15 of the European Convention on Human Rights, nevertheless expressed 'very great doubt' whether it threatened the life of the nation and referred to the 'faulty intelligence assessments' prior to the Iraq war.[183] In his speech Lord Hoffmann was more candid still, referring to 'the widespread scepticism which has attached to intelligence assessments since the fiasco over Iraqi weapons of mass destruction'.[184] Nonetheless, the constitutional objection to the judiciary over-ruling the government on matters of national security relied on by the majority of the judges in the *Bellmarsh* decision in holding that they could not question the government's assertion that there existed a public emergency.

74 The loosening of the deference doctrine has encouraged a flood of actions in the regular courts (in addition to challenges in the IPT) against the intelligence services arising from alleged abuses in the "War against Terror" and involving the question of intelligence cooperation with international partners.[185] These include a challenge to the legality of the ministerial guidance issued to cover the conduct of intelligence officers dealing with intelligence partners, who have suspects in detention,[186] to the alleged supply of location information by GCHQ to the US for overseas drone attacks,[187] and to the alleged involvement of MI6 with US authorities in an alleged rendition.[188]

75 In a number of instances lawyers representing litigants claiming to have suffered human rights abuses at the hands of foreign intelligence services have brought proceedings against UK authorities for disclosure of any related intelligence they may have received from the services in the counties accused of wrongdoing that could assist the claim in foreign courts.[189] This strategy was used in *Binyam Mohammed*[190] and several other prominent cases.[191] *Binyam Mohammed* was brought by a former Guantanamo Bay detainee to force the Foreign Secretary to disclose potentially exculpatory material, based on reports from the US Government to MI5 and MI6, concerning his alleged torture in Pakistan. He had also been rendered by the US to Morocco and tortured there. After protracted litigation the Court of Appeal confirmed that, notwithstanding

[183] Ibid., para. 154.

[184] ibid., para. 94.

[185] I. Leigh, 'National Courts and International Intelligence Cooperation' in H. Born, I. Leigh and A. Wills (eds.), *International Intelligence Cooperation and Accountability*, (Routledge, 2011) ; C. Murray, 'Out of the Shadows: the Courts and the United Kingdom's Malfunctioning Counter-Terrorism Partnerships', *Journal of Conflict & Security Law* 2013, 18(2), 193–232.

[186] *Equality and Human Rights Commission v Prime Minister* [2011] EWHC 2401 (Admin), [2012] 1 WLR 1389 (unsuccessful).

[187] *R (application of Khan) v Secretary of State for Foreign and Commonwealth Affairs* [2014] All ER (D) 112 (Jan); [2014] EWCA Civ 24. The legality of alleged passing by GCHQ to the US of locational information to CIA for drone attacks in Pakistan unsuccessfully challenged because the court refused to make a declaration that would involve judging the acts of a sovereign foreign government (the USA) and because of the hypothetical nature of the alleged criminality involving GCHQ officials.

[188] *Belhaj v Straw and others* [2017] UKSC 3, in which the Supreme Court held that action against UK officials for complicity in wrongdoing by US officials overseas was not barred by the doctrines of state immunity or foreign act of state.

[189] The so-called *Norwich Pharmacal* remedy (which takes its name from the case of *Norwich Pharmacal v Commissioners of Customs and Excise* [1974] AC 133) allows a litigant to seek disclosure of evidence from third parties to litigation in this way.

[190] *R (Binyam Mohammed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65.

[191] *Al Rawi and others v Security Service* [2011] UKSC 34.

the importance of intelligence cooperation, the public interest in discussion of allegations of complicity in torture outweighed the objections of the US authorities.[192]

II. Evidential protections and intelligence

1. Public interest immunity[193]

76 Traditionally the common law protected intelligence from examination in legal proceedings through the doctrine of public interest immunity in civil cases (the doctrine cannot be used in criminal cases). This allows for a minister to claim through a signed certificate that to allow the material covered by the certificate to be adduced would be contrary to the public interest. This procedure is controversial because the exclusion of secret material may effectively prevent individuals with a sound legal claim against the government for alleged wrongs by intelligence agencies/officials from pursuing them because of suppression of available evidence for essentially procedural reasons. Although at one time these certificates were treated as conclusive by the courts, the modern practice allows the court to inspect the contested material and weigh the claim against other interests, ordering disclosure if it so chooses.[194] Where the court finds that exclusion is justified there is the reassurance that the secrecy claim has been confirmed by an independent body. If, on the other hand, the challenge to the certificate is upheld it may lead to the government seeking to settle or discontinue proceedings to avoid complying with an adverse judicial ruling to disclose intelligence considered to be damaging to national security.[195]

77 Public Interest Immunity has clear limitations, however, which have led in recent years to the devising of alternative means to protect intelligence material in litigation. The option of settling a claim to avoid disclosure in the event of an adverse judicial ruling is not a possibility, however, when the government is only a third party to litigation, joined because as an intelligence partner it may have relevant information relating to proceedings that are brought against foreign officials or agencies. This has been a partial explanation for the UK Government seeking to regain a measure of control by introducing Closed Material Procedures under the Justice and Security Act 2013 (described below). Moreover, exclusion of material prevents the government also from relying on it in order to defend or justify powers, such as executive measures based

[192] The High Court had initially acceded to the Foreign Secretary's request to maintain passages redacted from earlier judgments in the face of threats from the US to re-evaluate its intelligence sharing with the UK if these details (based on reports from the US government to MI5 and MI6 about Binyam Mohammed's treatment) were published: *R (Binyam Mohammed) v Secretary of State for Foreign and Commonwealth Affairs [2009] EWHC 152 (Admin).* The court later revisited its conclusion in the light of new information that became available: *R (Binyam Mohammed) v Secretary of State for Foreign and Commonwealth Affairs (No. 5)* [2009] EWHC 2549 (Admin).

[193] R. Glover, *Murphy on Evidence* (14th ed., Oxford 2015), Ch. 13; C. Forsyth, 'Public Interest Immunity: Recent and Future Developments' (1997) 56 *Cambridge Law Journal* 51; M. Supperstone, 'A New Approach to Public Interest Immunity?' [1997] *Public Law* 211; I. Leigh, "Reforming Public Interest Immunity", [1995] 2 *Web Journal of Current Legal Issues* http://www.bailii.org/uk/other/journals/WebJCLI/1995/issue2/leigh2.html ; I. Leigh and L. L Lustgarten, "Five Volumes in Search of Accountability: The Scott Report", (1996) 59 *Modern Law Review* 695–725; I. Leigh, 'Public Interest Immunity', (1997) *Parliamentary Affairs* 55–70; J. Jacob, "From Privileged Crown to Interested Public" [1993] *Public Law* 121; A. Tomkins,' Public Interest Immunity After Matrix Churchill' [1993] *Public Law* 650.

[194] *Conway v Rimmer* [1968] AC 910.

[195] As happened following the ruling of the UK Supreme Court in *Al-Rawi v The Security Service* [2011] UKSC 34; [2012] 1 AC 531 that the Security Service could not serve closed defences within a closed material procedure.

on intelligence material. The difficulties of devising a way in which it can do so consistently with fair trial rights (notably Art. 6 of the ECHR) have led to the creation of specialist court-substitute bodies which are not fully adversarial in the traditional sense. Foremost among these are the Investigatory Powers Tribunal (discussed above) and the Special Immigration Appeals Commission.

2. Special advocates

So far as practical and evidential difficulties of handling secret material in court are concerned, attitudes are now also more sceptical. The European Court of Human Rights has insisted that the right to a fair trial (Art. 6 ECHR) requires courts to accommodate some form of adversarial challenge to intelligence material even if normal trial procedures, such as full cross-examination, cannot apply.[196] This has led in recent years to procedural innovations such as the introduction of the Special Immigration Appeals Commission and, more widely, of Special Advocates who are security-cleared. These innovations provide for the limited introduction of intelligence into legal proceedings in a way consistent with fair trial rights: that is they allow some form of adversarial challenge to intelligence material even if normal trial procedures, such as full cross-examination, cannot apply. **78**

Prior to 1997, in immigration deportation cases, a decision to deport a person from the United Kingdom on grounds of national security was taken by the Home Secretary personally and there was no formal right of appeal. The Home Secretary's decision was reviewed by an Advisory Panel, which made recommendations on whether the Home Secretary's decision to should stand. The Panel's recommendations were purely advisory and although it was able to review the evidence relating to national security threat this material was not disclosed to the applicant or his legal representatives on grounds of national security. The decision of the European Court of Human Rights in *Chahal v. UK* that a person facing deportation on grounds of national security had to be given an effective means of challenging this before a judicial body[197] led Parliament to create the Special Immigration Appeals Commission (SIAC). SIAC is an independent judicial tribunal in which intelligence material can be presented with limited disclosure to the deportee. The legislation provides for a Special Advocate to represent an appellant in cases in which there is non-disclosable security evidence in relation to the immigration decisions of the Home Secretary.[198] Special Advocates have access to closed material and represent the deportee's interests but may not take instructions from the deportee.[199] Since their introduction the use of Special Advocates has spread to a number of other courts and tribunals in which decisions based on intelligence material can be challenged. **79**

Innovations like the Special Immigration Appeals Commission and Special Advocates are often regarded by practising lawyers as regrettable incursions into the principle of open justice.[200] In particular, critics point to the professional and ethical difficulties for **80**

[196] See discussion of the special advocate system and the Special Immigration Appeals Commission procedure in A and Others v UK Appl no. 3455/05, 19 February 2009 (G.C.), paras. 207–224 and drawing an analogy between the requirements of Art. 6 and the procedural requirements of Art. 5(4) ECHR.

[197] *Chahal v UK* (1997) 23 EHRR 413. The Court found that the then existing procedure violated Art. 5 (4) of the European Convention on Human Rights, because judicial review proceedings could not effectively review the grounds for his detention, and because he was not represented before the Advisory Panel.

[198] Special Immigration Appeals Commission Act 1997, S. 6.

[199] Special Immigration Appeals Commission Rules (as amended), Rules 36–38.

[200] C. Forcese and L. Waldman *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of "Special Advocates" in National Security Proceedings,* Ottawa 2007; Justice, *Secret Evidence* (London, 2009); M. Chamberlain, "Update on procedural fairness in closed

lawyers arising from the duty to represent the interests of a person from whom instructions cannot be taken and to whom material cannot be disclosed. Effectively Special Advocates reviewing security material work in isolation and without normal professional support. Subsequent decisions have produced minor changes to the process- notably the requirement that to satisfy the European Convention on Human Rights a person must be told the "gist" of the case against him- but in other respects the system has been found to be a necessary limitation on the right of fair trial.[201]

3. Closed material procedures

81 Faced with a growing number of legal challenges implicating the agencies the government sought to regain control and to establish a secure environment for litigation concerning security intelligence, by introducing Closed Material Procedures ('CMPs') in the Justice and Security Act 2013. The government argued that, on the one hand, disclosure of intelligence material in open court would endanger national security and intelligence cooperation but, on the other, to wholly exclude it would prevent judges from taking important material into account and hamper the government in fully defending itself against allegations (CMPs apply to civil cases only). The legislation is intended to allow intelligence material to be considered under conditions of secrecy, which may include consideration in the absence of the other party and their lawyers. The court releases a summary of closed proceedings but, exceptionally, even the fact that CMPs have been used may be withheld.

82 A number of safeguards are built into the legislation.[202] Before agreeing to the use of CMPs the court must be satisfied that that the alternative of an application for public interest immunity has been considered, that there is relevant material which if disclosed would damage national security and that a CMP would be in the interests of the fair and effective administration of justice. The court will consider the material provided in support of the application, to determine that it is relevant and that its disclosure would damage national security. The court is under a duty to review the lifting of CMPs in the light of developments throughout the proceedings.[203] Special advocates can be appointed to participate and to challenge the relevance and admissibility of the intelligence material.[204] Moreover, there is an obligation to report to Parliament annually on the operation of the CMP provisions[205] and for an independent five-year review of the legislation.[206]

83 CMPs are highly controversial as critics allege that they amount to a form of secret justice.[207] They argue that a civil claimant should not in effect have to bear the cost of

proceedings". (2009) 28(4) Civil Justice Quarterly 448–543; J. Jackson, "The Role of Special Advocates: Advocacy, Due Process and the Adversarial Tradition", (2016) 20(4) International Journal of Evidence and Proof 343–362.

[201] ECtHR, *Case of A. and Others v. The United Kingdom*, Application no. 3455/05, Judgment (Grand Chamber, 19 Feb. 2009), paras. 223 and 224, finding a violation of Article 5.4 because the applicants were hindered in challenging the decision to deport by the generalised nature of allegations against them.

[202] Justice and Security Act 2013, S. 6.

[203] Justice and Security Act 2013, S. 7.

[204] Justice and Security Act 2013, S. 9.

[205] Justice and Security Act 2013, S. 12.

[206] Justice and Security Act 2013, S. 13.

[207] For critical discussion of the 2013 Act see: A.Peto and A.Tyrie, *Neither Just Nor Secure* (Centre for Policy Studies, 2011) http://www.cps.org.uk/files/reports/original/130123103140-neitherjustnorsecure.pdf; A.Tomkins, "Justice and security in the United Kingdom" (2014) Israel Law Review. ISSN 0021-2237 http://eprints.gla.ac.uk/91090/1/91090.pdf; T. Hickman, 'Turning out the lights: the Justice and Security Act 2013' http://ukconstitutionallaw.org/2013/06/11/tom-hickman-turning-out-the-lights-the-justice-and-security-act-2013/.

protecting intelligence in the form of restrictions of his or her rights.[208] Some argue that it violates Article 6 ECHR,[209] but domestic courts have so far not found any incompatibility and the system has yet to be tested at Strasbourg.

4. Criminal trials and intelligence material

Until the 1990s intelligence was mainly used as background by prosecution authorities and it was unprecedented for intelligence officers to appear in court as witnesses. The more prominent role that MI5 in particular has in relation to counter-terrorism has brought about a significant change in that practice: it is now common for security officials to give evidence (often, at the judge's discretion, anonymously and from behind a screen to protect their identity from becoming public). At the same time, practice has changed to anticipate the disclosure of relevant intelligence material in criminal prosecutions. **84**

There are, nonetheless, a number of significant evidential restrictions, designed to give protection to intelligence material. Foremost among these is the prohibition on the use in legal proceedings of intercept material.[210] The ban has been regularly reviewed over the last three decades[211] but successive governments have chosen to retain it for operational reasons- it prevents any form of parallel challenge being mounted in criminal proceedings to the decision to intercept. Maintenance of the ban, however, puts the UK out of line with its international intelligence partners and now appears somewhat anomalous in view of the much greater transparency surrounding surveillance, following the introduction of the 2016 Act and the introduction of a judicial input to authorisation through the 'double lock' provisions. **85**

Where the prosecution relies on other intelligence material, this has to be disclosed to the defence- as noted above, Classified Material Procedures do not apply to criminal trials. It is, however, possible (though rare in practice) for parts of a criminal trial to be held in camera, with the public and press excluded.[212] Moreover, where intelligence material forms part of the background to a prosecution but is not relied upon in evidence, the question arises of whether it should be disclosed to the defence. Prima facie, any unused material that might reasonably be considered to assist the accused's defence or to undermine the prosecution case must be disclosed under the procedures contained in the Criminal Procedure Investigations Act 1996.[213] The Act provides however that material is not subject to this duty where it would be against the public interest to disclose it[214] and, in such cases for the prosecution to apply to the court for a determination. **86**

[208] See Justice, Justice and Security Green Paper Consultation Response (London, 2012); Liberty, Liberty's Response to the Ministry of Justice's Green Paper- Justice and Security (London, 2012); Human Rights Joint Committee, 24th Report for 2011–12, The Justice and Security Green Paper, HL 286/HC 1777 (2011–12).

[209] John Sullivan, "Closed Material Procedures and the Right to a Fair Trial" , 29 Maryland J. Int'l Law 269 (2014). Available at: http://digitalcommons.law.umaryland.edu/mjil/vol29/iss1/12.

[210] The current provision is the Investigatory Powers Act 2016, S. 56.

[211] See I. Leigh, 'Intelligence and the Law in the United Kingdom' in L. Johnson (ed.), *Oxford Handbook of National Security Intelligence*, (Oxford University Press, 2010), 654–55.

[212] For one example in which the Court of Appeal upheld the restrictions (which effectively prevented any reporting of the circumstances surrounding the terrorism charges in question, of which the defendant had been acquitted) see *Guardian New and Media Ltd v.R and Erol Incedal* [2016] EWCA Crim 11.

[213] Criminal Procedure Investigations Act 1996, S. 3(1).

[214] Criminal Procedure Investigations Act 1996, S. 3(6). Exceptionally, the prosecution may apply ex parte to the court to determine if disclosure would be contrary to the public interest. The courts have given guidance to protect the right of fair trial in such circumstances, including in some instances the appointment of a special advocate to contest the prosecution's application for withholding disclosure: *R v. H; R v. C* [2004] UKHL 3.

G. Conclusion

87 The environment in which the security and intelligence agencies operate has undergone rapid change in the past quarter century. This period has seen the agencies move from their Cold War orientation to preoccupation with a diverse range of threats, especially international terrorism, but also proliferation threats and organised crime. It has also seen a remarkable growth in transparency. In the 1980s the agencies were still shrouded in secrecy, so much so that one of them (MI6) was not even officially acknowledged. Now, on the other hand, the system of accountability to the parliamentary Intelligence and Security Committee is well-established, the services have a relatively public profile (through their websites, and the heads give public lectures and occasional media interviews) and they recruit staff openly, to the extent of championing employment diversity.

88 So far as legal developments are concerned the change has been no less dramatic. Since 9/11 the courts have become accustomed to hearing claims against the security and intelligence agencies arising from the alleged abuses of the "War on Terror" and have, to a small degree at least, relaxed their previously deferential attitude to national security. The government, in turn, has accepted that intelligence cannot simply be a "no-go zone" for legal accountability. Although protective measures like the Investigatory Powers Tribunal, Special Advocates and Closed Material Procedures are controversial for their incursion on the principles of open and adversarial justice, they do at least allow independent courts and tribunals to examine the actions of the security and intelligence agencies in a way that was unimaginable not so long ago.

89 Most dramatic of all perhaps has been the technological change over the period, with many of the capabilities of the agencies laid bare since 2013 by the unprecedented disclosures of Edward Snowden. The result was a (long overdue) public and parliamentary debate about surveillance, resulting, with the Investigatory Powers Act 2016, in a detailed and comprehensive legal framework that regulates and gives legitimacy to the agencies' capabilities. These changes have important implications for oversight of the agencies also, bringing a discernible shift towards expert oversight through the new office of the Investigatory Powers Commissioner.

90 Technology also poses constant challenges, especially through the rapidly escalating cyber threat, both from hostile states, such as North Korea and Russia, and non-state actors. There has been a discernible attempt both to educate public opinion[215] and to legitimise the work of GCHQ especially in this field, through the establishment of a public-facing National Cyber Security Centre.[216]

91 Looking ahead, the international environment for the agencies work will continue to evolve, especially following Brexit in March 2019. Since 9/11 international intelligence cooperation in the fight against terrorism has grown exponentially and although for the UK agencies these arrangements are very far from exclusive to EU partners, those relationships are nonetheless important, not least in sharing information about foreign terrorist fighters and other violent Islamists. Significantly, early in 2018 the Chief of MI6

[215] See especially the Prime Minister's Mansion House speech in November 2017 to accusing Russia of mounting 'a sustained campaign of cyber espionage and disruption' and of seeking to 'weaponise information' by planting fake news stories and photo-shopped images 'in an attempt to sow discord in the West and undermine our institutions': Rt. Hon. Theresa May, Mansion House Speech, 13 November 2017: https://www.gov.uk/government/speeches/pm-speech-to-the-lord-mayors-banquet-2017.

[216] https://www.ncsc.gov.uk/.

appeared alongside the heads of the DGSE and BND to affirm the importance of continued cooperation after the UK leaves the EU[217] and the Prime Minister spoke at the same security conference of the aspiration for a new post-Brexit security treaty between the EU and the UK.[218]

---

[217] Joint statement 16th February 2018, 'BND, DGSE and MI6 emphasise necessity of international cooperation' http://www.bnd.bund.de/EN/_Home/Startseite/Buehne_Box/Textbausteine/News_ENG/180216_MSC18/180216_MSC18_Artikel.html;jsessionid=09F8AA7423E566CB6008DD5085713E84.1_cid386?nn=3132246.

[218] 'Theresa May: "Europe's Security is our Security', BBC News 17 February 2018. http://www.bbc.co.uk/news/av/uk-politics-43096450/theresa-may-europe-s-security-is-our-security.