DIETRICH / EIFFLER (Hrsg.)

Handbuch des Rechts der Nachrichtendienste

Handbuch des Rechts der Nachrichtendienste

herausgegeben von

Prof. Dr. Jan-Hendrik Dietrich
Hochschule des Bundes

Dr. Sven-R. Eiffler
Ministerialrat im Bundeskanzleramt

bearbeitet von

Dr. Josephine Asche
Eberhard Karls Universität Tübingen

Dr. Christian Bareinske, LL.M.
Geschäftsbereich Bundeskanzleramt

Dr. Peter Bartodziej
Bundeskanzleramt

Prof. Dr. Jochen von Bernstorff, LL.M.
Eberhard Karls Universität Tübingen

Dr. Karsten Brandt
Bundesministerium des Innern

Dr. Phillip Brunst
Cybercrime Research Institute Köln

Prof. Dr. Jan-Hendrik Dietrich
Hochschule des Bundes für öffentliche Verwaltung

Dr. Sven-R. Eiffler
Bundeskanzleramt

Prof. Dr. Klaus Ferdinand Gärditz
Rheinische Friedrich-Wilhelms-Universität Bonn

Dr. Michael Greßmann
Bundesministerium der Justiz und für Verbraucherschutz

Prof. Dr. Christoph Gusy
Universität Bielefeld

Prof. Dr. Jan Hecker, LL.M.
Bundeskanzleramt

Sebastian Hinüber, LL.M.
Bundeskanzleramt

Prof. Dr. Reinhard Klaushofer
Universität Salzburg

Prof. Dr. Wolfgang Krieger
Philipps-Universität Marburg

Prof. Dr. Julian Krüper
Ruhr-Universität Bochum

Dr. Gregor Kutzschbach
Bundesministerium des Innern

Prof. Dr. Klaus von Lampe
John Jay College of Criminal Justice New York

RiLG Dr. Markus Löffelmann
Landgericht München I

Prof. Dr. Nele Matz-Lück, LL.M.
Christian-Albrechts-Universität zu Kiel

Simon McKay, Barrister
University of Leeds

OStA beim BGH Stephan Morweiser
Generalbundesanwalt beim Bundesgerichtshof

Dr. Oliver Rüß
Bundesministerium des Innern

Prof. Dr. Samuel Salzborn
Justus-Liebig-Universität Gießen

Dr. Thomas Siems, LL.M.
Geschäftsbereich Bundesministerium der Verteidigung

Prof. Dr. Clive Walker
University of Leeds

Dr. Gunter Warg, Mag. rer. publ.
Hochschule des Bundes für öffentliche Verwaltung

RiOVG Dr. Holger Wöckel
Oberverwaltungsgericht für das Land Nordrhein-Westfalen

Philipp Wolff
Bundeskanzleramt

BOORBERG

Bibliografische Information der Deutschen Nationalbibliothek | Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über www.dnb.de abrufbar.

ISBN 978-3-415-05921-4

Lektorat: Rechtsanwalt Dr. Arnd-Christian Kulow, Stuttgart | Herstellung: Dipl.-Wirt.-Ing. (FH) Melanie Wanderer, Stuttgart | Satz: Thomas Schäfer, www.schaefer-buchsatz.de | Druck und Bindung: Beltz Bad Langensalza GmbH, Neustädter Straße 1–4, 99947 Bad Langensalza

Richard Boorberg Verlag GmbH & Co KG | Scharrstraße 2 | 70563 Stuttgart
Stuttgart | München | Hannover | Berlin | Weimar | Dresden
www.boorberg.de

Vorwort

Nachrichtendienste stehen im Fokus kritischer Öffentlichkeit. Viel wird über ihre Arbeit geschrieben, viel wird über sie diskutiert. Dabei fällt auf, dass sich die fachwissenschaftliche Auseinandersetzung mit dem Thema Nachrichtendienste, jedenfalls in Deutschland, auf wenige Werke und nur einzelne Autoren beschränkt. Dies gilt insbesondere für die rechtswissenschaftliche Begleitung der öffentlichen Diskussion.

Mit dem Handbuch des Rechts der Nachrichtendienste wird nun erstmals eine umfassende, systematische Bearbeitung des für Nachrichtendienste geltenden Rechtsregimes geboten. Es eignet sich als grundlegendes Nachschlagewerk für Wissenschaft, Rechtsprechung, Verwaltung, Politik und Medien. Schwierige nationale, europarechtliche und völkerrechtliche Rechtsfragen werden problemorientiert unter Berücksichtigung dynamischer sicherheitsrelevanter Entwicklungen (z.B. Proliferation, Terrorismus, Wirtschaftsspionage oder Cyberangriffe) vertieft. Der aktuelle wissenschaftliche Diskurs über Auftrag, Befugnisse und Kontrolle von Nachrichtendiensten sowie die damit verbundene gegenwärtige Rechtspraxis, einschließlich der einschlägigen Rechtsprechung, werden umfassend dokumentiert und kritisch analysiert. Ein vergleichender Blick gilt dem Recht der Nachrichtendienste in Großbritannien und Österreich. Durch die Einbindung von Autorinnen und Autoren aus Wissenschaft, Justiz und Verwaltung liegt ein fundiertes, unabhängiges Gesamtwerk vor, das bewusst verschiedene, mitunter divergierende Ansichten in Bezug auf nachrichtendienstrechtliche Fragen zulässt. Jeder Beitrag gibt jeweils die persönliche Auffassung der Autorin bzw. des Autors wieder und steht nicht für die Institution, aus der sie/er stammt, wenngleich es die Absicht ist, dass in jeden Text die Erfahrungen und Kenntnisse aus dem beruflichen Hintergrund seiner Verfasserin bzw. seines Verfassers einfließen.

Jedem, der in den vergangenen Jahren an der Erstellung dieses Bandes mitgewirkt hat, ist v. a. eines deutlich geworden: Das Recht der Nachrichtendienste ist eine äußerst dynamische Rechtsmaterie, die ständigen Änderungsprozessen unterworfen ist. Während der Entstehung des Buches mussten deshalb beständig Gesetzesnovellen eingearbeitet, neue Judikate berücksichtigt oder neue Beiträge im Schrifttum gewürdigt werden. Den Autorinnen und Autoren des Handbuchs sind die Herausgeber vor diesem Hintergrund für die große Geduld und die Bereitschaft verbunden, bereits finalisierte Manuskripte mehr als nur einmal anzupassen. Dank schulden die Herausgeber insbesondere auch Herrn Dr. *Arnd-Christian Kulow* und Frau *Melanie Wanderer* vom Boorberg-Verlag für die umsichtige Betreuung und Unterstützung des Projekts.

München und Berlin im April 2017

Jan-Hendrik Dietrich Sven-R. Eiffler

Inhaltsverzeichnis

Neunter Teil
Regulierung nachrichtendienstlicher Tätigkeit im Ausland

§ 2
Legal regulation of intelligence services in the United Kingdom

Simon McKay and Clive Walker

Table of contents

Bibliography: This listing is selective – it does not reproduce all the sources in the hundreds of footnotes in this paper but instead seeks to provide selective leading commentaries.

Printed materials: Aldrich, R., *GCHQ* (Harper Collins, London, 2010); Allason, R., *The Branch: A History of the Metropolitan Police Special Branch 1883–1983* (Secker & Warburg, London, 1983); Anderson, D., *A Question of Trust – Report of the Investigatory Powers Review* (Home Office, London, 2015); Andrews, C., *The Defence of the Realm: The Authorized History of MI5* (Allen Lane, London, 2009); Bochel, H. et al., *'New Mechanisms of Independent Accountability': Select Committees and Parliamentary Scrutiny of the Intelligence Services* (2015) 68 *Parliamentary Affairs* 314; Bonino, S., and Kaoullas, L.G., 'Preventing Political Violence in Britain: An Evaluation of over Forty Years of Undercover Policing of Political Groups Involved in Protest' (2015) *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2015.1059102; Bonner, D., *Executive Measures, Terrorism and National Security* (Ashgate, Aldershot, 2007); Born, H. et al. (eds.), *International Intelligence Cooperation and Accountability* (Routledge, Abingdon, 2012); Born, H., Johnson, L., and Leigh, I, (eds.) *Who's Watching the Spies. Establishing Intelligence Service Accountability* (Potomac, Dulles, 2005); Butler, R., *Review of Weapons of Mass Destruction* (2003–04 HC 898); Cabinet Office, *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees* (London, 2010); Cabinet Office, *Securing Britain in an Age of Uncertainty – The Strategic Defence and Security Review* (Cm.7948, London, 2010); Cabinet Office, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald* (London, 2015); Cabinet Office, *Tackling extremism in the UK* (London, 2013); Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London, 2011); Cobain, I., *Cruel Britannia: A secret history of torture* (Portobello Books, London, 2012); Creedon, M., *Operation Herne. Part One Use of Covert Identities* (MPS, London, 2013); Davies, P.H.J., *MI6 and the Machinery of Spying* (Frank Cass, London, 2004); Davis, F., McGarrity, N., and Williams, G., *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, Abingdon 2014); de Silva, D., *The Report of the Patrick Finucane Review*, (2012–13 HC 802, 2012) paras.21–26; Defty, A., 'Educating

Parliamentarians about Intelligence: The Role of the British Intelligence and Security Committee' (2008) 64 *Parliamentary Affairs* 621; Defty, A., et al., 'Tapping the telephones of Members of Parliament' (2014) 29 *Intelligence and National Security* 675; Dorril, S., *MI6: Inside the Covert World of Her Majesty's Secret Intelligence Service* (Simon & Schuster, New York, 2000); Ellison, M., *The Stephen Lawrence Independent Review: Possible corruption and the role of undercover policing in the Stephen Lawrence case,* (2013–14 HC 1038); European Commission For Democracy Through Law (Venice Commission), *Report on the Democratic Oversight of the Security Services* (CDL-AD(2007)016, Strasbourg, 2007) and *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies* (CDL-AD(2015)006, Strasbourg, 2015); Evans, R., and Lewis, P., *Undercover: The True Story of Britain's Secret Police* (Faber & Faber, London, 2013); Foreign & Commonwealth Office, *Torture and Mistreatment and Reporting Guidance* (London, 2011) and *Overseas Security and Justice Assistance Guidance* (London, 2014); Gibson, P., *Review of Intercepted Intelligence in relation to the Omagh Bombing of 15 August 1998* (Northern Ireland Office, Belfast, 2009); Gibson, P., *The Report of the Detainee Inquiry* (Cabinet Office, London, 2013); Greenwald, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books, New York, 2014); Haggerty, K.D., and Ericson, R.V., 'The surveillant assemblage' (2000) 51 *British Journal of Sociology* 605; Her Majesty's Inspector of Constabulary (HMIC)*, A Review of National Police Units which provide intelligence on criminality associated with protest* (Home Office, London, 2012); Home Affairs Select Committee, *Undercover Policing: Interim Report* (2012–13, HC 837); Home Office, Communications Data Bill 2012 (Cm.8359, London, 2012); Home Office, *Countering International Terrorism* (Cm.6888, London, 2006); Home Office, *Departmental Committee on section 2 of the Official Secrets Act 1911* (Cmnd. 5014, London, 1972); Home Office, *Guidelines on Special Branch Work in the United Kingdom* (London, 2004); Home Office, *Intercept as Evidence* (Cm.8989, London, 2014); Home Office, *Intercept as Evidence* (Cm.7760, London, 2009); Home Office, *Reform of section 2 of the Official Secrets Act 1911* (Cmnd. 7285, London, 1978); Home Office, *Reform of section 2 of the Official Secrets Act 1911* (Cm. 408, London, 1988); Home Office, *Report of the Official Account of the Bombings in London on the 7th July 2005* (2005–06 HC 1087); Home Office, *Serious and Organised Crime Strategy* (Cm.8715, London, 2013); Home Office, *The Interception of Communications in Great Britain* (Cmnd.7873, London, 1980); House of Commons Constitutional Affairs Committee, *The Operation of the Special Immigration Appeals Commission (SIAC) and the Use of Special Advocates* (2004–5 HC 323-I); House of Commons Home Affairs Committee, *A Surveillance Society?* (2007–08 HC 58) and *Government Reply* (Cm.7449, 2008); House of Commons Home Affairs Committee, *Special Branch* (1984–85 HC 71); Hyland, K., and Walker, C., 'Undercover policing and underwhelming laws' [2014] *Criminal Law Review* 555; Independent Police Complaints Commission, *Ratcliffe-on-Soar Power Station (Operation Aeroscope) Disclosure Nottinghamshire Police* (London, 2012); Information Commissioner, *A Report on the Surveillance Society* (Wilmslow, 2006); Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies*, (Cm.8514, London, 2013); Intelligence and Security Committee, *Inquiry into Intelligence, Report into the London Terrorist Attacks on 7 July 2005* (Cm 6785, London, 2005) and Government Reply (Cm 6786, London, 2006); Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (2014–14 HC 1075); Intelligence and Security Committee, *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (2014–15 HC 795); Interception of Communications Commissioner's Office, *Inquiry into the use of Chapter 2 of Part I of the Regulation of Investigatory Powers Act (RIPA) to Identify Journalistic Sources* (London,

2015); Jeffery, K., *MI6: The History of the Secret Intelligence Service 1909–1949* (Bloomsbury, London, 2010); Joint Committee on Human Rights, *Allegations of UK complicity in torture* (2008–09 HL 152/HC 230) and *Government Reply* (Cm 7714, London, 2009); JUSTICE, *Intercept Evidence: Lifting the Ban* (London, 2006); JUSTICE, *Under Surveillance*, (London, 1998); Kirk-Smith, M., and Dingley, J., 'Countering terrorism in Northern Ireland: the role of intelligence' (2009) 20 *Small Wars and Insurgencies* 551; Leigh, I., and Lustgarten, L., 'The Security Commission' [1991] *Public Law* 215; Leigh, I., 'Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11' (2012) 27 *Intelligence and National Security* 722.; Lyon, D., *Surveillance Society* (Open University, Buckingham, 2001); Martin, G., Scott Bray, R., and Kumar, M., *Secrecy, Law and Society* (Routledge, Abingdon, 2015); Masferrer, A., and Walker, C., (eds.), *Counter-Terrorism, Human Rights and the Rule Of Law* (Edward Elgar, Cheltenham, 2013); McKay, S., *Covert Policing: Law and Practice*, (2nd ed., Oxford University Press, Oxford, 2015); Ministry of Justice, *Justice and Security Green Paper* (Cm.8194, London, 2011); Moran, J., 'Evaluating Special Branch and the use of informant intelligence' (2010) 25(1) *Intelligence and National Security* 1; Moran, J., *From Northern Ireland to Afghanistan* (Ashgate, Farnham, 2013); O'Floinn, M., and Ormerod, D., 'Social networking sites, RIPA and criminal investigations' [2011] *Criminal Law Review* 766; Phillips, D., Caless, B., and Bryant, R., 'Intelligence and its application to contemporary policing' (2007) 1(4) *Policing* 439; Phythian, M., 'The British Experience with Intelligence Accountability' (2007) 22 *Intelligence and National Security* 75; Prime Minister, *National Security Strategy and Strategic Defence and Security Review 2015* (Cm.9161, London, 2015); *Privy Council Review of intercept as evidence* (Cm.7324, London, 2008); Rose, C., *Ratcliffe-on-Soar Power Station Protest: Inquiry into Disclosure* (CPS, London, 2011); Tomkins, A., 'Justice and Security in the United Kingdom' (2014) 47 *Israel Law Review* 305; Walker, C., 'Intelligence and Anti-terrorism Legislation' (2005) 44 *Crime, Law and Social Change* 387; Walker, C., 'Keeping control of terrorists without losing control of constitutionalism' (2007) 59 *Stanford Law Review* 1395; Walker, C., *Terrorism and the Law* (Oxford University Press, Oxford, 2011); Walker, C., *The Anti-Terrorism Legislation* (3rd ed., Oxford University Press, Oxford, 2014); Walker, C., 'The governance of the Critical National Infrastructure' [2008] *Public Law* 323; Wright, P., *Spycatcher* (Heinemann, Sydney, 1987).

Internet sites (last viewed 05.10.2016): Centre for the Protection of National Infrastructure ('CPNI'), https://www.cpni.gov.uk/; Communications-Electronics Security Group ('CESG'), http://www.cesg.gov.uk/; Government Communications Headquarters ('GCHQ'), http://www.gchq.gov.uk/; Independent Reviewer of Terrorism Legislation, https://terrorismlegislationreviewer.independent.gov.uk/; Information Commissioner's Office, https://ico.org.uk/; Intelligence and Security Committee, http://isc.independent.gov.uk/; Intelligence Services Commissioner's Office, http://www.intelligencecommissioner.com/; Interception of Communications Commissioner's Office, http://www.iocco-uk.info/; Investigatory Powers Tribunal, http://www.ipt-uk.com/; Joint Intelligence Committee, https://www.gov.uk/government/organisations/national-security/groups/joint-intelligence-committee; Joint Terrorism Analysis Centre ('JTAC'), https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/joint-terrorism-analysis-centre.html; Metropolitan Police Service, Counter Terrorism Command, http://content.met.police.uk/Article/Counter-Terrorism-Command/1400 006569170/1400006569170; National Counter Terrorism Security Office, https://www.gov.uk/government/organisations/national-counter-terrorism-security-office; National Crime Agency, http://www.nationalcrimeagency.gov.uk/; National Security Council, https://www.gov.uk/government/organisations/national-security/groups/national-security-council; Office of Surveillance Commissioners, https://osc.independent.gov.

uk/; Secret Intelligence Service, https://www.sis.gov.uk/; Security Service (MI5), https://www.mi5.gov.uk/; Special Immigration Appeals Commission, https://www.gov.uk/guidance/appeal-to-the-special-immigration-appeals-commission; Surveillance Camera Commissioner, https://www.gov.uk/government/organisations/surveillance-camera-commissioner.

A. The institutions of intelligence services in the UK: current format and history

The purpose of this paper is to analyse critically the legal regulation of the intelligence services in the United Kingdom.[1] Given that the said services have existed for many decades and enjoy a rich history which includes responses to colonial conflicts,[2] the breakup of Ireland and continuing political violence in Northern Ireland,[3] two World Wars and the Cold War, and contemporary terrorism, all alongside incursions from inquisitive or hostile foreign states, our task is impossible to achieve in depth. Therefore, our plan is as follows. In this introductory part, the three main intelligence institutions and their current statutory frameworks will be delineated. The second section of the paper will examine the functions of the intelligence services. The third, and most complex, part of the paper will consider their powers. The fourth part will deal with potential liabilities, both criminal and civil. The fifth part will consider the mechanisms for oversight. The conclusions in the sixth part will take stock and consider challenges and proposals for reform. This paper was updated to 1 January 2016, but some brief comments were added later about the Investigatory Powers Bill which became the Investigatory Powers Act 2016. **1**

I. Institutions

There are three major intelligence institutions.[4] The objectives for all are set by the government paper, *Securing Britain in an Age of Uncertainty – The Strategic Defence and Security Review*; the highest priority risks were international terrorism, cyber-attacks, international military crises, and major civil emergencies[5] Additional strategic statements have been devised for terrorism,[6] cyber-threats,[7] **2**

1 The focus is on by far the largest jurisdiction, England and Wales. Scotland and Northern Ireland are distinct but share the same intelligence agencies and many of the same laws (but see Regulation of Investigatory Powers (Scotland) Act 2000 (asp 11)).

2 Thomas, M., *Empires of Intelligence: Security Services and Colonial Disorder After 1914* (University of California, Berkeley, 2007); Walton, C., *Empire of Secrets: British Intelligence, the Cold War and the Twilight of Empire* (Harper, London, 2013).

3 See McMahon, P., *British Spies and Irish Rebels: British Intelligence and Ireland, 1916–1945* (Boydell Press, Woodbridge, 2008); Moran, J., *From Northern Ireland to Afghanistan* (Ashgate, Farnham, 2013).

4 See especially Andrews, C., *The Defence of the Realm: The Authorized History of MI5* (Allen Lane, London, 2009); Jeffery, K., *MI6: The History of the Secret Intelligence Service 1909–1949* (Bloomsbury, London, 2010); Aldrich, R., *GCHQ* (Harper Collins, London, 2010).

5 Cm.7948, London, 2010. There is an updated version: Prime Minister, National Security Strategy and Strategic Defence and Security Review 2015 (Cm.9161, London, 2015).

6 Home Office, *Countering International Terrorism* (Cm.6888, London, 2006), as revised. See Walker, C., *The Anti-Terrorism Legislation* (3rd ed., Oxford University Press, Oxford, 2014) chap. 1.

7 Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London, 2011).

and organized crime.[8] The National Security Council, chaired by the Prime Minister, was established in 2010 to oversee all aspects of this strategy.[9] In 2012, the Prime Minister appointed a **National Security Adviser** with responsibility for co-ordinating and delivering the Government's international security agenda. Another important top-level forum, for officials rather than Ministers, is the **Joint Intelligence Committee ('JIC')**, which is part of the **Cabinet Office** and provides Ministers and senior officials with intelligence assessments based on reports from the various agencies.[10] The work of both the Joint Intelligence Committee and National Security Council is assisted by the **Joint Intelligence Organisation ('JIO')**, which comprises assigned intelligence analysts. It drafts assessments and forwards them to the Joint Intelligence Committee.[11]

3 The foremost domestic intelligence agency is the **Security Service**, commonly known by one of its historical titles as **MI5** (Military Intelligence, Section 5). The spectre of German spies in the early 20th century accounted for its formation (and that of the Secret Intelligence Service, described next). It is headed by the Director General and has a staff of around 4,000 (representing a threefold increase since 2001).[12] As well as the headquarters in London, since 2005, eight regional offices have been established in Britain, additional to a headquarters in Northern Ireland. The 'Single Intelligence Account' for all agencies in 2014–15 was £ 1.9bn (€ 2.58bn).[13]

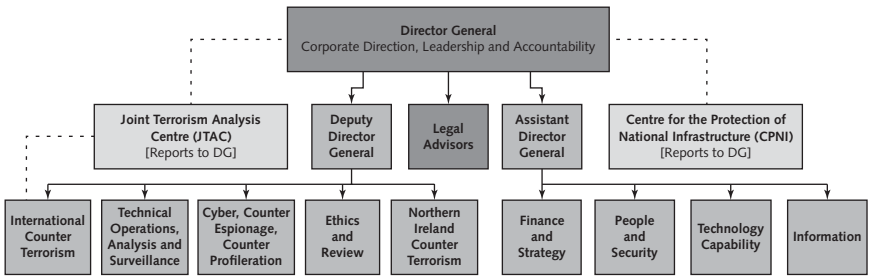

Diagram: Organisation of the Security Service[14]

4 Out of the nine activities in the diagram above, by far the most prominent is counter-terrorism; international terrorism accounts for 65% of overall expenditure, while Northern Ireland-related terrorism takes up another 15%.

5 Analysis and assessment of terrorist threats is monitored by the **Joint Terrorism Analysis Centre ('JTAC')**, established administratively and without any

8 See Home Office, *Serious and Organised Crime Strategy* (Cm.8715, London, 2013).

9 https://www.gov.uk/government/organisations/national-security/groups/national-security-council.

10 https://www.gov.uk/government/organisations/national-security/groups/joint-intelligence-committee.

11 https://www.gov.uk/government/organisations/national-security/groups/joint-intelligence-organisation.

12 See *Walker* and *Staniforth*, 'The amplification and melding of counter-terrorism agencies: from security services to police and back again') in Masferrer and Walker (eds.), *Counter-Terrorism, Human Rights and the Rule Of Law* (Edward Elgar, Cheltenham, 2013)

13 HM Treasury, *Spending Round 2013* (Cm.8639, London, 2013) p. 54.

14 Source: https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management.html.

specific legal basis in 2003.[15] It is based in the Security Service but also draws on expertise from sixteen sources in the police, government departments, and intelligence agencies so as to ensure collaboration and sharing in the products of intelligence and thereby reducing the dangers of cross-agency competition and suspicion, as had sometimes arisen in Northern Ireland between the police and security services.[16] JTAC analyses and assesses intelligence, from which it publishes threat levels[17] as well as issuing secret warnings and reports to its security and governmental 'customers'. Thus, it operates at a much higher level than 'fusion centers' in the USA and so has avoided the imposition of major organisational change at a time of crisis.[18]

6 Protective security advice is given a public interface through the **Centre for the Protection of National Infrastructure ('CPNI')**. The national infrastructure consists of key assets which are vital to the continued delivery and integrity of essential services, but there is no statutory basis either for this definition or the CPNI.[19] The CPNI has links to a network of police Counter Terrorism Security Advisors who are in turn supported by the National Counter Terrorism Security Office (NaCTSO). This police unit, operated through the National Police Chiefs' Council, concentrates on planning and protective security against terrorism. The primary role is to provide help, advice and guidance to specified sectors – not only the critical national infrastructure but also operators of crowded places, hazardous sites, and dangerous processes, as well as individuals whose personal security is at risk.[20]

7 Counter-espionage (such as by Russia and China, and especially through cyber techniques) and counter-proliferation remain important tasks for the Security Service. In the past, subversion was a major concern, but has waned following the end of the Cold War, though 'counter-extremism' is an emerging aspect of counter-terrorism.[21]

8 The Security Service Act 1996 permitted Security Service involvement in supporting police investigations of serious organised crime in 1996, but, this activity was suspended in 2006 so as to allow concentration on counter-terrorism,[22] and the work is now transacted by the police-led National Crime Agency.[23]

15 See Intelligence and Security Committee, *Annual Report 2003–04* (Cm.6240, London, 2004) para.92 et seq; https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/joint-terrorism-analysis-centre.html.

16 The alleged distrust had led to the appointment of a special adviser, former MI6 Director, Sir Maurice Oldfield, in 1979: Hansard (House of Commons) vol.975 col.1096 Humphrey Atkins, 11 December 1979; *Jeffrey*, 'Security policy in Northern Ireland' (1990) 2 *Terrorism & Political Violence* 21; *Kirk-Smith* and *Dingley*, 'Countering terrorism in Northern Ireland: the role of intelligence' (2009) 20 *Small Wars and Insurgencies* 551.

17 https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html.

18 For criticism of this system, see *German* and *Stanley*, *Fusion Center Update* (ACLU, Washington DC, 2007); US Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Federal Support for and involvement in State and Local Fusion Centers* (2012). FBI involvement is described in 9/11 Review Commission, *The FBI: Protecting the Homeland in the 21st Century* (Washington DC, 2015).

19 See *Walker*, 'The governance of the Critical National Infrastructure' [2008] *Public Law* 323.

20 https://www.gov.uk/government/organisations/national-counter-terrorism-security-office.

21 See Cabinet Office, *Tackling extremism in the UK* (London, 2013).

22 http://news.bbc.co.uk/1/hi/uk/4760273.stm.

23 See Crime and Courts Act 2013, Pt.I; http://www.nationalcrimeagency.gov.uk/

9 The **Secret Intelligence Service ('SIS')** (historically **MI6**) handles foreign threats to national security. It is based in London and is headed by the Chief. The SIS concentrates on threats with an international aspect, especially terrorism, proliferation and espionage, challenges to UK defence, foreign policies, and economic well-being, and serious crime. Two important parameters of its work have long been, first, bilateral intelligence relationships with the US and the **'Five Eyes'** arrangements for the sharing of intelligence (also with Australia, Canada and New Zealand),[24] and, second, supporting the diplomatic and military effort in conflicts. The SIS is much more coy about its structure compared to the Security Service. However, academic analysis has suggested that it involves a 'Production' side, which mounts operations from resident stations abroad (often at embassies) in response to demands laid upon it by a tasking 'Requirements' side which then collates and disseminates the intelligence gathered to SIS customers in government and other security agencies.[25] The context for these activities is set by a much stronger **Ministerial (political) tasking** of the SIS than for the Security Service, as a reflection of the greater political and diplomatic factors associated with overseas operations:

'The Foreign Secretary said: "We task them all the time and I discuss with [the Chief of SIS] and with the director of GCHQ on an almost continuous basis their work. So I think, you know, how they allocate their resources is very much guided by us in the Foreign Office. I would say it's set by us predominantly, the overall oversight of these Agencies and their overall strategy is set by us." The Home Secretary made clear that the relationship with the Security Service is quite different. … The view of successive governments has been that the Security Service should be free from political direction. There is, therefore, less scope for reprioritising at a strategic level – whether by the Home Secretary or the NSC. The Home Secretary explained: "I think it is important that there is an operational independence …"'[26]

10 The third major security agency is the **Government Communications Headquarters (GCHQ)**. GCHQ grew out of the expansion of signals interceptions and encryption in wartime, with the initial Government Code and Cipher School being set up in 1919. Its specialist task remains to handle intelligence and security aspects of signals surveillance. Most GCHQ officers are based in Cheltenham, though facilities also exist at various military outposts, especially in Cyprus and the Ascension Island. It contains the largest number of staff of all the main agencies (around 6,000 officers, compared to 4,000 for the Security Service and 3,000 for the SIS),[27] and is headed by a Director. Its work falls principally in three areas: the cyber threat; terrorism; and serious crime.[28] CESG (Communications-Electronics Security Group) is a unit within GCHQ which provides security assistance to government communications systems and pri-

24 See British-US Communication Intelligence Agreement 5 March 1946 (National Archives HW/80/4).

25 See *Dorril*, *MI6: Inside the Covert World of Her Majesty's Secret Intelligence Service* (Simon & Schuster, New York, 2000); Davies, P.H.J., *MI6 and the Machinery of Spying* (Frank Cass, London, 2004). For an illustration, see *Butler*, *Review of Weapons of Mass Destruction* (2003–04 HC 898).

26 Intelligence and Security Committee, *Annual Report 2011–2012* (Cm.8403, London, 2012) paras.26, 27.

27 Intelligence and Security Committee, *Annual Report 2012–2013* (2013–13 HC 547) para.121.

28 http://www.gchq.gov.uk/what_we_do/the-threats-we-face/Pages/index.aspx.

vate operators of Critical National Infrastructure; it also operates as the UK National Technical Authority for information assurance, including cryptography.[29]

The field of state intelligence activities is far from wholly occupied by the foregoing three agencies. Constraints on space rule out a full description of all other operators. However, two have particular importance. **11**

First, **Defence Intelligence** is part of the Ministry of Defence and furnishes defence-related intelligence principally to the Ministry of Defence and the Armed Forces.[30] It consists of both military and civilian research staff. Its head is the Chief of Defence Intelligence, who reports to the Chief of the Defence Staff and the Permanent Secretary of the Ministry of Defence. The total staff is around 4,000, based in the UK and overseas. The largest element is the **Joint Forces Intelligence Group** which was established in 2012 under the Joint Forces Command. **12**

As well as defence-related intelligence, there is also police intelligence work, which in the field of national security took the form of the 'Irish Special Branch' which was founded in 1883.[31] The Police Special Branch units in the 43 constabulary areas in England and Wales have traditionally concentrated on extremism, terrorism, and security from external threats especially at ports and airports. Much of its work has now shifted to more specialist policing bodies,[32] the largest contingent of which consists of the specialist counter-terrorism policing network, headed by a Senior National Co-ordinator (Counter Terrorism) and a National Coordination Centre which supports the work of the **Counter-Terrorism Command in the Metropolitan Police Service** (combining in 2006 its Special Branch and Anti-Terrorist Squad).[33] There are now four regional Counter Terrorism Units and a further five **regional Counter Terrorism Intelligence Units**, established as a response to the 7 July 2005 transport attacks in London and as pursuing the aims of concentrating expertise, fostering greater collaboration with the security agencies, and achieving better national coverage and local contacts by opening provincial offices.[34] In total, they involve around 6,000 officers and 2,000 civilian staff and thereby represent the most important structural innovation in the contemporary era.[35] The CTUs and CTIU are not the same as 'fusion centres' since they do not involve the fusion of personnel, but they are designed to secure co-working through co-location. **13**

29 http://www.cesg.gov.uk/Pages/homepage.aspx.

30 See https://www.gov.uk/government/groups/defence-intelligence; Intelligence and Security Committee, *Annual Report 2011–2012* (Cm. 8403, London, 2012) para.174.

31 See Allason, R., *The Branch: A History of the Metropolitan Police Special Branch 1883–1983* (Secker & Warburg, London, 1983); House of Commons Home Affairs Committee, *Special Branch* (1984–85 HC 71); Home Office, *Guidelines on Special Branch Work in the United Kingdom* (London, 2004); Metropolitan Police, *Special Branch: Introduction and Summary of Responsibilities*, http://www.met.police.uk/foi/pdfs/other_information/borough/so12_introduction.pdf, 2004.

32 See further Staniforth, A., *Blackstone's Counter-Terrorism Handbook* (Oxford University Press, 2009) ch 3.

33 http://content.met.police.uk/Article/Counter-Terrorism-Command/1400006569170/1400006569170

34 See Home Office, *Pursue, Prevent, Protect, Prepare* (Cm 7547, 2009) para.8.10.

35 Anderson, D., *The Terrorism Acts in 2011* (Home Office, 2012) para.2.42.

II. Statutory framework

14 The statutory framework now establishing the three intelligence agencies is of remarkably recent origins despite the lengthy histories previously indicated. MI5's existence was not legally acknowledged until the Security Service Act 1989, when section 1 laconically stated that 'There shall continue to be a Security Service …'. MI6 and GCHQ were constituted in the same vein by the Intelligence Services Act 1994 ('ISA 1994'). They follow a similar and relatively curt structure. Likewise, it was not until the 1980s and 1990s that the use of general and intrusive surveillance techniques began to be enshrined in a formal legal framework via the agency legislation mentioned above, as well as by the **Interception of Communications Act 1985**, the **Police Act 1997**, and the **Regulation of Investigatory Powers Act 2000 ('RIPA 2000')**.[36]

15 These changes were driven more by the deficiencies in technical legality (the problem that there was no legal basis) rather than deficiencies in structures, functions, powers, or oversight. Therefore, the legislation sought to entrench rather than to alter contemporary practices. Any shortcomings had been reluctantly recognized and were attributable to several exogenous influences.

16 First, there were legal influences. A repeated reminder of defects came from the European Court of Human Rights ('ECtHR'), though it was often a lack of 'accordance with the law' which was the stumbling block rather than any substantive failure to accord sufficient respect for rights such as privacy. This criticism was sustained against the interception of communications procedures in *Malone v United Kingdom*,[37] In *Hewitt and Harman v United Kingdom*[38] and *Esbester v United Kingdom,*[39] the applicants argued successfully that the absence of any statutory basis for the activities of the intelligence services violated Article 8 of the European Convention on Human Rights ('ECHR'). Anticipation of further such challenges before the UK courts, as enabled by the Human Rights Act 1998 ('HRA 1998'), accelerated the passage of the most comprehensive statutory reform, the RIPA 2000.

17 Second, the UK experienced no intelligence scandals on a scale akin to the US COINTELPRO affair,[40] but some revelations did cause disquiet. Amongst the most prominent were the 'Zircon affair' in 1987, in which a secret British spy satellite programme was revealed,[41] and, around the same time, the 'Spycatcher affair' – the memoirs of former MI5 agent, Peter Wright, who alleged that 'For five years we bugged and burgled our way across London at the State's behest, while pompous bowler-hatted civil servants in Whitehall pretended to look the

36 Wadham, J, 'The Intelligence Services Act 1994' (1994) 57 *Modern Law Review* 916; Leigh, I., 'Accountability of Security and Intelligence in the United Kingdom' in Born, H., Johnson, L., and Leigh, I, (eds.) *Who's Watching the Spies. Establishing Intelligence Service Accountability* (Potomac, Dulles, 2005).

37 App. no.8691/79, Ser A 82 (1984) para.80. See Akdeniz, A., Taylor, N., and Walker, C., 'Regulation of Investigatory Powers Act 2000 (1): BigBrother.gov.uk: State surveillance in the age of information and rights' [2001] *Criminal Law Review* 73.

38 App. no.12175/86, (1992) 14 EHRR 657.

39 App no.18601/91, (1993) 18 EHRR CD 72.

40 See Church Committee, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities* (United States Senate, 94th Congress, 2nd Session, 1976).

41 Bradley, A.W., 'Parliamentary privilege and the Zircon affair' [1987] *Public Law* 1 and 'Parliamentary privilege, Zircon and national security' [1987] *Public Law* 488.

other way.'[42] More recently, the excessive activities of undercover officers have also been viewed as disreputable.[43]

B. Functions of the intelligence services: legal duties

Indications have already been given of the intended missions and practical focus of work of each agency as well as, belatedly, their statutory frameworks. The purpose of this section of the paper is to explore the functions in those frameworks. **18**

The functions of the Security Service are set out in section 1(2) to (4) of the Security Service Act 1989 (as amended)[44] and comprise: **19**

(2) … the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. (3) It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands. (4) It shall also be the function of the Service to act in support of the activities of the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

'Terrorism' is **broadly defined** in the **Terrorism Act 2000**, section 1.[45] 'Serious crime' is defined by section 81(3) of the RIPA 2000 as one where a person with 'no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more; [or where] the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose'.[46] Regarding economic well-being, a precise definition is resisted but will be affected by Directive 97/66/EC which requires a link to national security if personal data is affected.[47] It has been held in *C v Police and Secretary of State*[48] that relatively modest sums of money could be involved. However, the key term, 'national security' is not defined comprehensively here, though there are some partial judicial explanations in other contexts.[49] The term has been held to be sufficiently precise for the purposes of the ECHR.[50] **20**

42 Wright, P., *Spycatcher* (Heinemann, Sydney, 1987) p. 54

43 See Evans, R., and Lewis, P., *Undercover: The True Story of Britain's Secret Police* (Faber & Faber, London, 2013).

44 See ISA 1994, s.1; Security Service Act 1996; Crime and Courts Act 2013, s.61.

45 See Walker, C., *The Anti-Terrorism Legislation* (3rd ed., Oxford University Press, Oxford, 2014) chap.1.

46 For preventing and detecting, see s.81(5).

47 Intelligence and Security Committee, *Annual Report 2005–2006* (Cm.6864, London, 2006) para.97.

48 IPT/03/32/H, 14 November 2006.

49 See *Secretary of State for the Home Department v Rehman* [2001] UKHL 47*; R (Secretary of State for the Home Department) v Information Commissioner* [2006] EWHC 2958 (Admin); *Case C-524/06 Huber v Bundersrepublik Deutschland* [2008] ECR I-9705; *Kennedy v United Kingdom* App. no.26839/05, 18 May 2010.

50 *Harman and Hewitt v United Kingdom (no.2)* App no 20371/92, 1 September 1993; *Christie v United Kingdom*, App no. 21482/93, 78 –A DR 119 (1994); *Kennedy v United Kingdom*, App no.26839/05, 18 May 2010.

21 The **functions of the Secret Intelligence Service** are set out in section 1 of the **ISA 1994**:

'(1) There shall continue to be a Secret Intelligence Service … under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be

(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

(b) to perform other tasks relating to the actions or intentions of such persons.

(2) The functions of the Intelligence Service shall be exercisable only

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom; or

(c) in support of the prevention or detection of serious crime.'

22 The phrase the 'British Islands' means the United Kingdom, the Channel Islands and the Isle of Man.[51]

23 The functions of GCHQ are set out in section 3(1) of the ISA 1994:

'(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be

(a) 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; and

(b) to provide advice and assistance about (i) languages, including terminology used for technical matters, and (ii) cryptography and other matters relating to the protection of information and other material,

to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

(2) The functions referred to in subsection (1)(a) above shall be exercisable only

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) 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; or

(c) in support of the prevention or detection of serious crime.'

51 Interpretation Act 1978, Schedule.

The various statements of functions reflect major deficiencies.[52] Many of the key terms are left chronically vague. Furthermore, other than the statements in the 1994 Act that the activities should relate to the actions or intentions of 'persons outside the British Islands' (confined to economic well-being in the case of GCHQ), there is there is very little guidance as to the relationships between the agencies as to their overlapping functions and therefore the potential for destructive rivalry. Finally, the other important intelligence agencies in the defence and police sectors are not mentioned at all and continue to have no specific statutory basis. **24**

C. Legal regulation of activities

Many of the daily activities of the security agencies are left unregulated by law. Key issues of targeting, processing, and liaison with other agencies at home and abroad are doubtless the subject of internal governance but little is disclosed to the public[53] and even less is set in legal format. Details have very exceptionally been revealed – for instance, in connection with the 7/7 London Bombings (2005) and the murder of Lee Rigby (2013).[54] What the law does seek to regulate are those activities which are likely to infringe individual rights. Therefore, this third part of the paper will consider the legal powers which have been granted and whether they sufficiently recognise the rights and interests of individuals.[55] **25**

I. Property interferences

The need for statutory authorisations of what would otherwise amount to civil law trespass to property, criminal damage, and other interferences with proprietary interests,[56] by the intelligence services was made manifest following the decisions in *Harman* and *Esbester*. The ISA 1994 created a framework for legality but did not confront the legal implications of surveillance conduct. The RIPA 2000 has since complemented its provisions permitting interference with property by creating an authorization and approval regime for surveillance activity. The **Code of Practice on Covert Surveillance and Property Interference 2014**[57] issued under RIPA 2000, section 71, provides further guidance, but guidance about some aspects of the ISA 1994 (especially its impact on external communications) was not brought forward until the Equipment Interference **26**

52 See further Leigh, I., 'Accountability of Security and Intelligence in the United Kingdom' in Born, H., L Johnson and Leigh, I. (eds.) *Who's Watching the Spies. Establishing Intelligence Service Accountability* (Potomac, Dulles, 2005); Phythian, M., 'The British Experience with Intelligence Accountability' (2007) 22 *Intelligence and National Security* 75; Born, H. et al. (eds.), *International Intelligence Cooperation and Accountability* (Routledge, Abingdon, 2012).

53 An exception is the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees* (Cabinet Office, London, 2010).

54 See Home Office, *Report of the Official Account of the Bombings in London on the 7th July 2005* (2005–06 HC 1087); Intelligence and Security Committee, *Inquiry into Intelligence, Report into the London Terrorist Attacks on 7 July 2005* (Cm 6785, London, 2005) and Government Reply (Cm 6786, London, 2006); Intelligence and Security Committee, *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (2014–15 HC 795).

55 The materials are based on those in McKay, S., *Covert Policing* (2nd ed., Oxford University Press, Oxford, 2014).

56 See Wireless Telegraphy Acts 1949 and 1967.

57 See for all the RIPA 2000 Codes, https://www.gov.uk/government/collections/ripa-codes.

Code of Practice was proposed in 2015.[58] An authorization is not necessary: for entry 'into areas open to the public in shops, bars, restaurants, hotel foyers, blocks of flats or any other premises to which, with the implied consent of the occupier, members of the public are afforded unqualified access'; or for entry on any other land or premises at the invitation of the occupier.[59] It is possible to obtain consent for entry by deception, but an authority is necessary.[60] The draft Code also avows the use by the intelligence services of computer network exploitation, more commonly referred to as "hacking", using the provisions in the ISA 1994 as the legal basis for doing so.

27 The relevant provisions which govern the property interference activities of the three major intelligence agencies of the ISA 1994 are sections 5 and 6. The police are subject to a more stringent regime under the Police Act 1997, Part III.[61] Section 5(1) of the ISA 1994 provides that no interference with property (which might include land or personal property such as briefcases or vehicles) or wireless telegraphy will be unlawful provided it is authorized by a **warrant issued by the Secretary of State** (a senior government Minister – usually the Home Secretary for the Security Service or the Foreign Secretary for the other agencies). A warrant may be issued in respect of any property or wireless telegraphy[62] if the Minister thinks it is necessary[63] for the purposes of assisting the agencies in the discharge of their statutory functions.[64] Before a warrant can be issued, the Secretary of State must be satisfied that the interfering conduct to be engaged in is proportionate to what it seeks to achieve.[65] This requires an assessment of whether what it is thought may be achieved by engaging in the conduct 'could reasonably be achieved by other means'.[66] A warrant can only be issued by the Secretary of State unless the case is urgent, in which case a less senior Minister must have expressly authorized it to be issued and a statement to this effect is endorsed on the warrant by a senior official.[67] There are provisions for the issuance of a warrant in urgent cases.[68]

28 The SIS and GCHQ may not obtain a warrant in respect of property within the British Islands,[69] since the Security Service has domestic primacy. Where the Security Service is acting in support of a law enforcement agency in the prevention and detection of serious crime, a warrant must not be issued where it relates to property in the British Islands, unless it amounts to serious crime. However, the Security Service may make an application for a warrant authorizing action to be taken on behalf of either of the other agencies.[70] If issued, the Security Service's functions may be extended to include those of the other

58 See Hansard (House of Lords) vol.767 col. 147, 7 December 2015.
59 Code of Practice on Covert Surveillance and Property Interference 2014, para.7.4.
60 *Ibid*., para.7.4
61 See Carter, P.B., 'Evidence obtained by the use of a covert listening device' (1997) 113 *Law Quarterly Review* 467.
62 ISA 1994, s.5(2)
63 ISA 1994, s.5(2) (a)
64 ISA 1994, s.5(2) (i)-(iii)
65 ISA 1994, s.2(b).
66 ISA 1994, s.(2A) as amended by RIPA 2000, s. 74.
67 ISA 1994, s.6(1).
68 ISA 1994, s.6(1) (c)
69 ISA 1994, s.3.
70 Code of Practice, para.7.36.

agency if the activities authorized would otherwise fall within their statutory functions.[71]

Unless renewed, a warrant lasts for six months[72] and may be renewed by the Secretary of State.[73] If granted on an urgent basis, it ceases to have effect after the end of the fifth working day following the day of issue.[74] A warrant must be cancelled once the Secretary of State is satisfied that the conduct authorized is no longer necessary.[75] **29**

The ISA 1994, section 7, makes provision for an authorisation to be given by the Secretary of State **for acts committed outside the UK** where the person would otherwise be liable in the United Kingdom under the criminal or civil law of any part of the United Kingdom (including the general liability of Crown servants under section 31 of the 1948 Criminal Justice Act). As a result, agents involved in bugging, burglary, or bribery may be excused from any legal consequences under UK law if duly authorised. Such activities remain illegal both under the laws of the country of commission and under international law. The latter may mean that section 7 could still provide a 'licence to kill' but probably not a licence to torture.[76] **30**

II. Interception of communications

Another highly intrusive form of surveillance is the reading of another person's messages. Building on legislation dating from 1985,[77] RIPA 2000, Part I, Chapter 1, authorises the interception of communications, supplemented by the Code of Practice for the Interception of Communications 2010. **31**

A communication is intercepted in the course of its transmission by means of a telecommunication system if, and only, if a person (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of that system, or (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents available, while being transmitted, to a person other than the sender or intended recipient of the communication.[78] The definition of 'telecommunications system' is set out in section 2(1) of RIPA 2000.[79] The term 'in the course of its transmission' is not defined. **32**

The meaning of 'modification' for the purposes of the section is extrapolated in section 2(6) and includes the attachment of any apparatus to, or other modification of or interference with, any part of the system or any wireless telegraphy apparatus used for making transmissions to or from apparatus comprised in the system. Such modification must occur in the course of transmission, so the attachment of a device that records conversation after it has been transmitted, **33**

71 ISA 1994, s.4. But see further s.5.

72 ISA 1994, s.6(2)(a).

73 ISA 1994, s.6(3).

74 ISA 1994, s.6(2)(b).

75 ISA 1994, s.6(4).

76 ISA 1994, s.7.

77 See Interception of Communications Act 1985; *Report of the Committee of Privy Councillors appointed to inquire into the interception of Communications* (Cmnd.283, London, 1957).

78 RIPA 2000, s.2(2).

79 See further RIPA 2000, 2(8A) as amended by s.5 of the Data Retention and Investigatory Powers Act 2014 ('DRIPA 2014').

even by a fraction of a second, it not a modification.[80] However, modification can occur any time the telecommunications system is used for storing the communication for collection or access by the recipient and for later collection.[81] Thus, the storage of the message during transmission does not end transmission, and it is even not relevant that it may already have been listened to at the time of interception.[82] The Court of Appeal has held that 'the first receipt of the communication should not be considered as bringing the transmission to an end', a ruling which impinged on journalists who hacked into the voicemail accounts of mobile phone users.[83]

34 The **Directive on Privacy and Electronic Communications**, 2002/58/EC of 12 July 2002[84] extended the protection under Article 8 of the European Convention, by requiring express legal authority for interceptions and other surveillance activities. The Court of Appeal rejected in 2005 the contention that the Directive required a more expansive interpretation of the definition of 'interception'.[85] The Directives were reconsidered in *R v Coulson and Kuttner*,[86] the Crown arguing that the concept of transmission for the purposes of section 2 (7) went further than that envisaged by the Directives.[87] In the event, the Court declined to decide the issue.[88]

35 This interpretation **raises questions of legal certainty**. In *Liberty and others v United Kingdom*,[89] the ECtHR considered the previous statutory regime under the Interception of Communications Act 1985 and sustained an adverse finding against the United Kingdom. It is equally unclear whether the RIPA 2000 meets the ECtHR's standard of specification required in the warrant for the interception of external communications.[90] In *R v Coulson and Kuttner*,[91] the Court of Appeal summarily dismissed the defence submission that the provisions lacked legal certainty. However, this issue of legal certainty is at the heart of a further Strasbourg application by Big Brother Watch and others.[92]

36 Without an authorisation, an offence of unlawful interception is potentially committed under section 1. However, there are some exceptions. First, section 3 of RIPA 2000 allows for lawful interception without an interception warrant where the sender and recipient consented to the interception.[93] If one party or intended party to the communication has consented and the appropriate sur-

80 *R v E* [2004] EWCA Crim 1243; *R v Allsopp* [2005] EWCA Crim 703.

81 RIPA 2000, s.2(7), (8).

82 *R v Coulson and Kuttner* [2013] EWCA Crim 1026.

83 *Ibid.*, para.27.

84 OJ L201, 31 July 2002 P. 0037–0047.

85 *R v Allsopp and others* [2005] EWCA Crim 703, para.46.

86 *R v Coulson and Kuttner* [2013] EWCA Crim 1026, paras.29–43.

87 *Marleasing SA v La Comercial Internacional de Alimentacion SA* [1990] ECR I-4135, para.8.

88 *R v Coulson and Kuttner* [2013] EWCA Crim 1026, para.39.

89 App. no.58243/00, 1 July 2008. See Goold, B., 'Liberty v United Kingdom: a new chance for another missed opportunity' [2009] *Public Law* 5.

90 See further *Kennedy v United Kingdom* App. no.26839/05, 18 May 2010; *Liberty v GCHQ* [2014] UKIPTrib 13_77-H; *Liberty v Secretary of State for the Foreign & Commonwealth Office* [2015] UKIPTrib 13–77-H; Murphy, M.H., 'Transparency and surveillance' [2006] *Public Law* 10.

91 [2013] EWCA Crim 1026, paras.44 and 45.

92 App. no.58170/13, 4 September 2013.

93 Section 3(1)(a) and (b).

veillance authorization has been put in place under Part II,[94] then the interception is not unlawful. Second, section 4 provides for lawful interception in some circumstances. Section 4(1) authorizes interception if it relates to communications of a person who either is, or who the interceptor has reasonable grounds for believing is, out of the country[95] and it relates to the use by persons of that country of either a public telecommunications service or what would amount to such if those to whom it was offered or provided to were members of the public within the United Kingdom.[96]

37 More clearly, interception of communications can be lawfully undertaken pursuant to a warrant issued by the Secretary of State in accordance with section 5 of RIPA 2000.[97] A warrant includes the power to authorize or require the person named in the warrant to make, in accordance with an international mutual assistance agreement a request for assistance for an interception,[98] the provision of intercepted communications to the foreign authorities.[99] The Secretary of State cannot issue an interception warrant **unless there is a belief** (which does not have to be based on reasonable grounds) that to do so would be necessary for the following aims and be proportionate to those aims: in the interest of national security, for the purpose of preventing or detecting serious crime, for the purpose of safeguarding the economic well-being of the United Kingdom, or for the purpose of giving effect to the provisions of any international mutual assistance agreement for the purpose of preventing or detecting serious crime. Where the warrant is necessary for the purpose of **safeguarding the economic well-being** of the United Kingdom, an amendment has been made by the Data Retention and Investigatory Powers Act 2014 ('DRIPA 2014'). This formula reflects Directive 97/66/EC, which permits lawful interception as a limit on data protection insofar as it relates to economic well-being of the state only where it relates to national security matters.[100]

38 So as to ensure the referencing up of this draconian power, a limited range of persons within the intelligence agencies may apply for an interception warrant. They are set out in section 6 of the Act and include the Director General of the Security Service, the Chief of the SIS, the Director of GCHQ, and the chief of Defence Intelligence. Only a limited number of police chief officers may apply.[101]

39 An interception warrant must be signed by the Secretary of State.[102] A senior official[103] may sign where the case is urgent and the issue of the warrant has been expressly authorized by the Secretary of State.[104] Section 8 of RIPA 2000

94 Such interceptions need to be supported by a directed surveillance authorization under RIPA 2000, s.29 (see below): s 3(2)(b).

95 RIPA 2000, s.4(1)(a).

96 RIPA 2000, s.4(1)(b).

97 RIPA 2000, s.5(1)(a).

98 RIPA 2000, s.5(1)(b).

99 RIPA 2000, s.5(1)(c) and (d).

100 Directive 97/66/EC, para.12. See further RIPA 2.000, s.5(4) and (5)

101 See Code of Practice, para.2.1. Applications may, however, be made by subordinates on their behalf provided they hold Crown office: ibid.

102 RIPA 2000, s.7(1)(a). By the Code of Practice, para.2.2, 'Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.'

103 RIPA 2000, s.7(1)(b).

104 RIPA 2000, s.7(2). For other formalities, see s.7(3)–(5).

governs the content of warrants. The *2013 Annual Report of the Interception Commissioner* describes 'essentially two types of warrants. Section 8(1) warrants and section 8(4) warrants'.[105] However, the warrants are in fact issued under section 5; section 8 regulates their content only. Section 5 warrants either authorize the interception of 'internal' or 'external' communications, and this categorisation affects what the warrant must in contain. It is important to note that only 'external' communications are defined in RIPA; by section 20, ,"external communication" means a communication sent or received outside the British Islands'. It follows that the interception of 'internal' communications does not necessarily mean that the interception does not take place outside the United Kingdom. 'Internal' for present purposes simply means not 'external' as the term is used in section 8(4) and defined in section 20.

40 A warrant in respect of internal communications must name or describe either one single person as the interception subject or a single set of premises where the interception is to take place.[106]The Code of Practice sets out further requirements for a warrant, including the operational background, the person or premises under surveillance, a description of the communications, and conduct to be undertaken.[107]

41 Under section 8(4)(a), the requirement to name a single person or premises does not apply to a warrant where the conduct authorized consists in the interception of 'external communications' or conduct authorized in relation to any interception by section 5(6) (described above). Subsection 4(b) also has the same effect if at the time of the issue of the warrant a ministerial certificate is also issued, specifying the descriptions of intercepted material the examination of which he considers necessary for the purposes of section 5(3)(a), (b), or (c).[108] The Secretary of State is the only official who can issue the certificate in such circumstances.[109] In every other respect, the nature of the warrant is the same. The effect of these provisions is the battleground for the **application to the ECtHR** following Edward Snowden's revelations of **systematic mass surveillance** and **data collection regimes** in the United States operating with the complicity of the United Kingdom, in the communicated case *Big Brother Watch and others v United Kingdom*.[110] The provisions in section 8(4) need to be read in conjunction with sections 15 and 16 (described below).

42 Sir Anthony May, the Interception Commissioner, has considered the operation of section 8(4):

'… any significant volume of digital data is literally useless unless its volume is first reduced by filtering. What is filtered out at this stage is immediately discarded and ceases to be available. What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process.'[111]

105 (2013–14 HC 1184) para.3.11; Code of Practice, paras.4.1–5.14.

106 RIPA 2000, s.8.

107 Code of Practice, para.4.2.

108 RIPA 2000, s.8(4)(b)(i) and (ii).

109 RIPA 2000, s.8(6).

110 App. no.58170/13, 4 September 2013.

111 (2013–14 HC 1184) para.6.5.40.

Though implying that large amounts of data are initially collected (mainly by GCHQ), the Commissioner concluded that in his judgment that no undue invasion of privacy was occurring.[112] For the most part, the UK's Investigatory Powers Tribunal (described later in the passage of this paper on 'Oversight') has also accepted the framework of restrictions and oversight as sufficient to safeguard human rights,[113] though it has also recently found some excessive usage contrary to articles 8 and 10 of the European Convention against foreign human rights organisations, raising again acute questions about the choice of targets as much as the execution of warrants which tends to be the focus of reviewers.[114] **43**

A **warrant** issued by the Secretary of State will last for **either three or six months** subject to it being cancelled or renewed. If it has been signed by the Secretary of State and endorsed with a statement that 'the issue of the warrant is believed to be necessary on grounds falling within section 5(3)(a) or (c)' but is not renewed, the relevant period means six months beginning with the day of the warrants issue.[115] A renewal for six months must be on the basis that it is necessary in the interests of national security or the protection of the economic well-being of the United Kingdom.[116] In all other cases (the prevention or detection of serious crime or for the purposes of giving effect to the provisions of any mutual assistance agreement), the time limit is three months.[117] A warrant issued by an official in urgent cases will cease to have effect after five days unless renewed.[118] There is no limit on the number of renewals, but a renewal must be made before the expiration of the existing warrant and other than in cases concerned with a mutual assistance agreement must be renewed under the hand of the Secretary of State[119] and only on the belief that it is necessary on the grounds upon which it was originally issued or one of the other grounds provided for in section 5(3).[120] **44**

Section 11 deals with the implementation of warrants, as amended by the DRIPA 2014. In summary, a warrant may be executed by the person to whom it is addressed and by any assistant served with a copy of the warrant.[121] It shall be the duty of those served who provide or control a postal or public telecommunications service (such as technicians) to give effect to the warrant[122] whether or not the person is in the United Kingdom,[123] although the duty does not extend to those steps not reasonably practicable to be taken.[124] A failure to comply is a criminal offence,[125] and the person's duty may also be enforceable by way of **45**

112 *Ibid.*, para.6.5.43.
113 See *Liberty v GCHQ* [2014] UKIPTrib 13_77-H; *Liberty v Secretary of State for the Foreign & Commonwealth Office* [2015] UKIPTrib 13–77-H.
114 *Liberty v GCHQ* [2015] UKIPT Trib 13 77-H 2.
115 RIPA 2000, s.9(6)(ab), as amended by the Terrorism Act 2006, s.32.
116 RIPA 2000, s.9(6)(b).
117 RIPA 2000, s.9(6)(c).
118 RIPA 2000, s.9(6)(a).
119 RIPA 2000, s.9(1)(b).
120 RIPA 2000, s.9(2).
121 RIPA 2000, ss.11 (2), 11(9).
122 RIPA 2000, s.11(4).
123 As amended by DRIPA 2014 2000, s.4(3).
124 RIPA 2000, s.11(5).
125 RIPA 2000, s.11(7).

injunction or specific performance of a statutory duty in Scotland.[126] This section has been amended by DRIPA 2014 where it relates to a person outside the United Kingdom. In determining whether the steps are reasonably practicable to take, regard must be had to any requirements or restrictions under the law of that country or territory relevant to the taking of those steps[127] and the extent to which it is reasonably practicable to give effect to the warrant in a way that does not breach any such requirements or restrictions.[128]

46 Several other new provisions were introduced by the DRIPA 2014 into section 11(2) relating to **extra-territoriality**. A warrant may now expressly be served under subsection (2) on a person outside the United Kingdom and may relate to conduct outside the jurisdiction.[129]

47 The provisions introduced by the **DRIPA 2014** are **designed to extend the obligations** to comply with warrants **on communications service providers** beyond the United Kingdom's borders. However, the incantation of all of this verbiage cannot overcome some basic facts of the communications service industry – that many external providers are based in the US and will generally be unwilling to comply without formal process under a laborious Mutual Legal Assistance Treaty which takes around 10 months to complete. A number of reports have commented on the practical difficulties in cases of terrorism,[130] and a special envoy, Sir Nigel Sheinwald, has made further proposals to try to short-circuit the legal processes.[131]

48 Sections 15 to 18 – 'restrictions on use of intercepted material etc' – raise further complications. Section 15 requires that the material from intercepts must not be disclosed beyond that which is necessary for the authorized purposes and must be destroyed once retention is no longer necessary. Section 15 (6) and (7) are interrelated and have implications for disclosure ('surrender') of intercept material to authorities 'of a country or territory outside the United Kingdom'. The effect is to require that the foreign country must have corresponding provisions.

49 Section 16 relates only to certified warrants under section 8(4) ('external communications') to ensure that the usage is necessary for the purposes for which the warrant was issued.[132] Intercept material falls within subsection (2) 'so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which' relates to a person who is at the material time in the British Islands and has as a purpose or one of its purposes identifying material in his communications, whether received or sent by him.[133] Subsection (3) pro-

126 RIPA 2000, s.11(8).

127 RIPA 2000, s.11(5A)(a).

128 RIPA 2000, s.11(5A)(b).

129 RIPA 2000, s.11(2A).

130 See Intelligence and Security Committee, *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (2014–15 HC 795); Anderson, D., *A Question of Trust – Report of the Investigatory Powers Review* (Home Office, London, 2015).

131 Cabinet Office, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald* (London, 2015). See further Cortes, S., 'Legalizing domestic surveillance' (2015) 22 *Richmond Journal of Law & Technology* 1; Global Network Initiative, *Data Beyond Borders* (Washington DC, 2015).

132 RIPA 2000, s.16(1)(a). The Interception of Communications Commissioner has condemned the 'convoluted language and style': (2013–14 HC 1184), para.6.5.33.

133 RIPA 2000, s.16(2)(a) and (b).

vides that included within this obscure definition is material that may in fact constitute that which has previously been excluded by the earlier provision if it is certified under section 8(4) and the material does relates only to communications sent during 'a period specified in the certificate that is no longer than the permitted maximum'.[134] The time period is six months in national security cases and three months in all other cases.[135]

50 The draft **revised Code of Practice** on the Interception of Communications issued in 2015 proposes some new paragraphs on safeguards in relation to warrants relating to external communications. These include a requirement of mandatory training, including specifically section 16.[136] Periodic audits are to take place, and there is a requirement to notify serious and non-serious breaches to senior management and the Interception Commissioner.[137]

51 Section 17, **'exclusion of matters from legal proceedings'**, is highly unusual in comparative law terms.[138] Section 17(1) prohibits, other than for the purposes of section 18, adducing evidence, asking questions, making a disclosure or assertion or doing any other thing for the purposes of, or in connection with, any legal proceedings or Inquiries Act 2005 proceedings[139] where the effect discloses or tends to disclose the contents of an intercepted communication or related communications data[140] or even the issuance of an intercept warrant. The extent of this prohibition on the use of intercept materials in court was examined in *Attorney General's Reference (No 5 of 2002).*[141] The question for the court was the tension between section 1(6) (which creates an exclusion from criminal liability for private side interception if the person who makes it is the person with a right to control the system or has the consent of that person) and section 18(4). The unanimous view of the (judicial) House of Lords was that section 17(1) did not preclude a forensic exploration of whether the telecommunications system was a public or private one. Where a determination was made that the system was a private one, the prohibition did not prevent a similar forensic exercise being embarked upon to ensure section 1(6) was complied with (in other words, that the interception was carried out by, or on behalf of, a person with the right to control the operation of the system).[142] The applicant in *Price v United Kingdom*[143] challenged the curtailment of the cross-examination of a witness because the prosecutor indicated that section 17 might apply. The trial judge from which the case arose had declined to rule on the effect on the fairness of the trial of section 17.[144] The European Court of Human Rights sub-

134 RIPA 2000, s.16(3)(a) and (b), as amended by the Terrorism Act 2006, s.32(6).

135 RIPA 2000, s.16(3A)(a) and (b).

136 Draft Code of Practice, para.6.4.

137 *Ibid.*, para.6.7.

138 See further Mirfield, P., 'Regulation of Investigatory Powers Act 2000: Part 2: Evidential Aspects' [2001] *Criminal Law Review* 91; Ormerod, D., and McKay, S., 'Telephone Intercepts and their admissibility' [2004] *Criminal Law Review* 15; JUSTICE, *Intercept Evidence: Lifting the Ban* (London, 2006); Horne, A., *The Use of Intercept Evidence in Terrorism Cases* (SN/HA/5249, House of Commons Library, London, 2011).

139 As amended by the Inquiries Act 2005, ss.48, 51, Sched.2, para.20(2).

140 RIPA 2000, s.17(1)(a).

141 [2004] UKHL 40.

142 *Attorney General's Reference* [2004] UKHL 40, para.22.

143 App. no.15602/07.

144 See *R v Price* [2009] EWCA Crim 2918.

sequently held that the article 6 challenge based on section 17 was inadmissible: "in the present case the applicant has not established that the alleged intercept evidence actually existed. Even if it did, it is difficult to point to any actual prejudice he might have suffered on account of its exclusion."[145]

52 Section 18 creates a number of **exceptions** to the section 17 prohibition. There were originally six categories of excluded proceedings, including proceedings for an offence under RIPA 2000 itself,[146] civil proceedings for a section 11(8) injunction, proceedings before the Investigatory Powers Tribunal, and proceedings relating to the Special Immigration Appeals Commission or the Proscribed Organisations Appeals Commission.[147] Several further proceedings have since been added, many consisting of specialist hearings relating to terrorism or financial sanctions.[148] In respect of these latter categories, disclosure is not capable of being made to the individuals concerned or their representatives[149] but can be disclosed to a special advocate.[150] Section 18(3) to (6) provide for other exceptions including disclosure of the contents of lawful interceptions and any part of legal proceedings for the purpose of determining whether they were in fact lawful. Section 18(7) envisages circumstances whereby a disclosure may be made during criminal proceedings to the judge conducting a criminal prosecution to enable him or her to ensure the fairness of the proceedings. A disclosure can also be made to a judge who orders disclosure to be made to him or her within criminal proceedings but only if satisfied that 'the exceptional circumstances of the case make the disclosure is essential in the interests of justice'.[151] Secondly, where the judge makes an order of disclosure to himself or herself, he or she may direct the prosecutor to make any admission of fact that the judge thinks is essential in the interests of justice.[152] Somewhat perversely, the judge can only make the order prior to seeing the relevant material, so presumably must rely on the prosecutor bringing it to the court's attention. In any event, having made the order, no further disclosure can be made to the defence, even if it is thought that it is in the interests of justice to do so.[153] In those circumstances, because of the statutory prohibition on disclosure, the prosecution may be discontinued as an abuse of process.

145 App. no.15062/07, 15 September 2016, para.102.

146 Or other relevant offence as defined in subsection 12 (a)–(j).

147 Special Immigration Appeals Commission Act 1997; Terrorism Act 2000, Sched.3. See further Walker, C., *Terrorism and the Law* (Oxford University Press, Oxford, 2011) chap. 6.

148 See s.18(1)(db)–(de).

149 Section 18(2).

150 For special advocates, see House of Commons Constitutional Affairs Committee, *The Operation of the Special Immigration Appeals Commission (SIAC) and the Use of Special Advocates* (2004–5 HC 323-I); Bonner, D., *Executive Measures, Terrorism and National Security* (Ashgate, Aldershot, 2007) ch 8; Ip, J., 'The rise and spread of the special advocate' [2008] *Public Law* 717; Chamberlain, M., 'Update on procedural fairness in closed proceedings' (2009) 28 *Civil Justice Quarterly* 448; Van Harten, G., 'Weaknesses of adjudication in the face of secret evidence' (2009) 13 *International Journal of Evidence & Proof* 1; *A v United Kingdom*, App no 3455/05, 19 February 2009, paras.219–20; Chedrawe, J., 'Assessing risk, minimising uncertainty, developing precaution and protecting rights' (2012) 12 *Oxford University Commonwealth Law Journal* 33.

151 RIPA 2000, s.18(7) and (8).

152 RIPA 2000, s.18(9).

153 RIPA 2000, s.17(10).

The *Attorney General's Guidelines: Section 18 RIPA*[154] offer advice to prosecutors regarding responding to questions about interception. Whether or not interception has taken place, the answer to the question should be along the lines of 'I am not in a position to answer that, but I am aware of sections 17 and 18 of the Regulation of Investigatory Powers Act 2000 and the Attorney General's Guidelines on the Disclosure of Information in Exceptional Circumstances under section 18.'[155] **53**

The **ban on the utilisation of intercepts** as evidence in most court processes has been a highly controversial policy. It has been the subject of repeated inquiries,[156] and the government initially committed itself to allowing wider forensic applications of intercepts.[157] However, an acceptable solution has proven elusive. In practice, the interests of the intelligence agencies have been prioritised. They have little interest in the costs and inconvenience of presenting their handiwork in court or being subject to the greater transparency which such testimony would entail. The **triumph of intelligence interests** was signalled by the Home Office in its paper, *Intercept as Evidence*,[158] concluding that no cost-effective system can be devised. **54**

Aside from the utilisation of intercepts of evidence, other controversies concern the choice of government ministers as the authorising authorities. In addition, no special laws protect especially sensitive data such as legally privileged materials or the communications of Members of Parliament,[159] though recent guidance on the latter demands extra caution by decision-makers.[160] **55**

III. Communications data

The acquisition and disclosure of communications data is confined to five dense sections of Part I, Chapter II of RIPA 2000, as amended by the DRIPA 2014.[161] There are two related Codes: the Code of Practice on the Acquisition and Disclosure of Communications Data, and the Code of Practice for the Reten- **56**

154 See further Crown Prosecution Service, *Disclosure Manual* (http://www.cps.gov.uk/legal/d_to_g/disclosure_manual/, 2005) chap. 27, Annex 1.

155 Attorney General's Guidelines, para.10.

156 See *Privy Council Review of the Anti-terrorism, Crime and Security Act* (2003–04 HC 100); Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning* (2006–07 HL 157/HC 394); *Privy Council Review of intercept as evidence* (Cm.7324, London, 2008); Home Office, *Intercept as Evidence* (Cm.7760, London, 2009); Gibson, P., *Review of Intercepted Intelligence in relation to the Omagh Bombing of 15 August 1998* (Northern Ireland Office, Belfast, 2009); Intelligence and Security Committee, *Annual Report 2009–2010*, (Cm.7844, London, 2010) paras.58–60, H.

157 Hansard (House of Commons) vol.471 col.959, 6 February 2008, Gordon Brown.

158 (Cm.8989, London, 2014).

159 See Defty, A., et al., 'Tapping the telephones of Members of Parliament' (2014) 29 *Intelligence and National Security* 675; *Lucas v Security Service* [2015] IPT/14/79/CH, 16 October 2015 Hansard (House of Commons) vol.600 col.694 19 October 2015.

160 See Hansard (House of Commons) The Wilson Doctrine: Written statement – HCWS291 4 November 2015, David Cameron. Blatant disregard for any privilege is revealed by HM Inspector of Prisons, *Prison Communications Inquiry* (London, 2015).

161 Note also the retention of communications data under Part 11 of the Anti-terrorism, Crime and Security Act 2001 which created a voluntary code on the retention of communications data but was superseded by arrangements under the EU Data Retention Directive (Directive 2006/24/EC), although the Directive has now been held to be invalid (*Digital Rights Ireland Limited v Minister for Communications*, C-293/12, 8 April 2014), as described below.

tion of Communications Data. Power-holders are defined in section 25(1) and include the intelligence agencies.

57 The legal implications arising from the acquisition and use of communications data are now under **serious challenge**; an application made by campaign group, Big Brother Watch, to the ECtHR following the Snowden leaks has been communicated[162] and Privacy International and others lodged complaints with the Investigatory Powers Tribunal.[163] The absence of previous domestic legal challenge is surprising, not least because an estimated 500,000 applications for authorizations are made every year[164], the majority of which derive from the Security Service.[165] The high number of authorizations is a matter about which the Interception of Communication Commissioner has expressed concern.[166]

1. Scope

58 Sections 21 and 22 relate to the acquisition and disclosure of 'data communications', section 23, the form and duration of authorizations, and section 24, payment to those required to comply with a notice. Section 25 deals with definitions and interpretation. Chapter II excludes any conduct that would amount to an interception of a communication under Chapter I but includes any conduct in relation to a postal service or telecommunication system for obtaining communications data and its disclosure to any person.[167] **'Conduct'** is defined in section 21(2) as conduct in which any person is authorized or required to engage by an authorization or notice granted or given under Chapter II and is in accordance with, or in pursuance of, the authorization or requirement.[168] It then amounts to 'lawful conduct' for the purposes of the subsequent provisions.

59 **'Data communications'** is defined in section 21(4). It can take a number of different forms, including traffic data 'comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted'.[169] Adding to the complexity, 'traffic data' is itself later defined in section 21(6) as data relating to the transmission of communications.

60 The **first category** of relevant data is that identifying, or purporting to identify, any person, apparatus or location to or from which the communication is, or may be, transmitted.[170] The Interception of Communications Commissioner describes it as 'data that may be attached to a communication for the purpose of transmitting it and could appear to identify the sender and recipient of the communication, the location … time … and other related data'.[171] The Code of Practice elaborates as follows:

---

162 *Big Brother Watch and others v United Kingdom*, App. no.58170/13.

163 IPT/13/93/CH.

164 Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies*, (Cm.8514, London, 2013) para.14.

165 *Ibid*., para.18.

166 *2013 Annual Report, of the Interception of Communications Commissioner* (2013–14 HC 1184), para.4.28

167 RIPA 2000, s.21(1).

168 RIPA 2000, s.21(2).

169 RIPA 2000, s.21(4)(a).

170 RIPA 2000, s.21(6)(a).

171 *2013 Annual Report of the Interception of Communications Commissioner* (2013–14 HC 1184), para.4.2.

'… [i]nformation tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records) … information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication … and … information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone).'[172]

The **second category** is data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted.[173] The Code of Practice simplifies this to 'identifies or selects, or appears to identify or select, transmission equipment'[174] and provides the following example: 'routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers-to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed).'[175] It also includes web browsing information but limited to 'the extent that only a host machine, server, domain name or IP address is disclosed'.[176] **61**

Category three is any 'data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication'.[177] The Code of Practice translates this as comprising: 'signals that activate equipment used, wholly or partially, for the transmission of any communication (such as data generated in the use of carrier pre-select or redirect communication services or data generated in the commission of, what is known as, 'dial through' fraud).'[178] **62**

The **final category** is 'any data identifying the data or other data as data comprised in or attached to a particular communication'.[179] This provision contains an additional qualification: 'but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.' The Code of Practice 'identifies data as data comprised in or attached to a communication. This includes data which is found at the beginning of each packet in a packet switched network that indicates which communications data attaches to which communication'.[180] **63**

In these ways, traffic data can include data identifying a computer file or a computer program to which access has been obtained, or which has been run, by means of the communication – but only to the extent that the file or program is identified by reference to the apparatus in which the file or program is stored. In relation to internet communications, it means traffic data stop at the apparatus within which files or programs are stored, so that traffic data may identify a **64**

172 Code of Practice, para.2.21.
173 RIPA 2000, s.21(6)(b).
174 Code of Practice, para.2.19.
175 Code of Practice, para.2.21.
176 Code of Practice, para.2.21.
177 RIPA 2000, s.21(6)(c).
178 Code of Practice, para.2.19.
179 RIPA 2000, s.21(6)(d).
180 Code of Practice, para.2.19.

server or domain name (web site) but not a web page.[181] It also includes any message written on the outside of a postal item, which is in transmission, may be content (depending on the author of the message) and fall within the scope of the provisions for interception of communications. For example, a message written by the sender will be content but a message written by a postal worker concerning the delivery of the postal item will not.[182] All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is traffic data within section 21(4)(a).[183]

65 Section 21(7) further defines traffic data 'comprising signals for the actuation of apparatus' as including references to any telecommunication system that the apparatus forms part of' and traffic data attached to a communication 'include references to the data and the communication being logically associated with each other'.[184]

66 Communications data obtained directly as a result of an interception warrant are 'related communications data' under section 20 of RIPA 2000 and therefore intercept product. It follows that any related communications data, and any other specific communications data derived directly from it, must be treated in accordance with the rules of retention and the restrictions on the use of intercepted material and related communications data.[185]

67 Communications data include any traffic data and any information other than the content of the communication apart from traffic data.[186] Data relating to the use made by any person of a postal or telecommunications service, or any part of it, known as 'service use information' fall within section 21(4)(b) of RIPA 2000.[187] The Intelligence and Security Committee defined it as 'information about a communication … [or] the information created when a communication takes place – for example the time and during of the contact'.[188] The Interception of Communications Commissioner preferred the 'who, when and where of a communication but not the content'.[189]

68 Communications data also include any information that is held or obtained, in relation to persons to whom service is provided by a person providing a postal service or telecommunications service.[190] This type of communications data is widely known as 'subscriber information' and relates to information held or obtained by a CSP about their customers and other users. This is a broad term and may include persons who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it. The Interception of Communications Commissioner described it as 'data held or obtained by a CSP in relation

181 Code of Practice, para.2.20.

182 RIPA 2000, s.21(7)(b)

183 Code of Practice, para.2.22.

184 RIPA 2000, s.21(7).

185 See further Code of Practice, para.1.11.

186 RIPA 2000, s.21(4).

187 Code of Practice, paras.2.23, 2.24.

188 Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies*, (Cm 8514, London, 2013), paras. 6, 7.

189 *2013 Annual Report, of the Interception of Communications Commissioner* (2013–14 HC 1184), para.4.2.

190 RIPA 2000, s.21(4)(c).

to a customer and may be the kind of information which a customer typically provides when they sign up to use a service'.[191]

69 Communications data are generated, held or obtained in the provision, delivery and maintenance of communications services. These are defined in sections 2(1) and 81(1) of RIPA 2000 as 'any service which consists in the collection, sorting, conveyance, distribution and delivery of postal items and is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items' or telecommunications service, defined as 'any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system'. **Telecommunications system** means 'any system which exists whether wholly or partly in the United Kingdom or elsewhere for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy'.

2. Key actors

70 The **Single Point of Contact ('SPoC')** officer is a creation of the Code of Practice and has a crucial role 'to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs'.[192] Where a relevant public authority does not have an SPoC or is 'unable to call upon the services' of one, they are prohibited under the Code of Practice from acquiring communications data.

71 The role of the SPoC is to promote 'efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken'.[193] The SPoC is supposed to provide some **objectivity** to the application and authorization process as well as advice to both the applicant and the designated person. The Code of Practice sets out no fewer than **nine functions** of an SPoC that range from engaging 'proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations' to advising 'applicants and designated persons on the interpretation of the [2000] Act', and providing 'assurance to designated persons that authorisations and notices are lawful under the Act and free from errors'.[194]

72 The Interception of Communications Commissioner reported in 2013 that the 'overall picture is that the SPoC process is a stringent safeguard' and acted 'to a good or satisfactory standard',[195] but in some cases they should 'exercise their guardian and gatekeeper role more robustly'.[196] The ISC has opined that SPoC's are 'trained to a high standard and take their responsibilities seriously and reject any applications that do not reach the required thresholds', although this assessment was based on evidence from the intelligence agencies.[197] Whether an SPoC is in fact equipped to advise meaningfully on complex legis-

191 *2013 Annual Report, of the Interception of Communications Commissioner* (2013–14 HC 1184), para.4.2. For examples, see Code of Practice, paras.2.16, 2.26.

192 Code of Practice, para.3.15.

193 Code of Practice, para.3.16.

194 Code of Practice, para.3.17.

195 *2013 Annual Report, of the Interception of Communications Commissioner* (2013–14 HC 1184) para.4.42(3).

196 *Ibid.,* para.4.42(2).

197 Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies* (Cm.8514, London, 2013) para.70.

lation, even after training, is **at least questionable**, although the Interception of Communications Commissioner reported in 2013 that 'SPoCs are scrutinizing and challenging applications [and] suggesting less intrusive or more effective ways that the applicant might meet their objective'.[198] However, it was also reported that backlogs were occurring due to a lack of staff or inadequate systems in the SPoC.[199]

73 Section 22 relates to the manner and grounds upon which communications data are obtained and disclosed. Section 22(1) creates 'a person designated' **('Designated Person')** and defined in section 25(2) as 'the individuals holding such offices, ranks or positions with relevant public authorities as are prescribed for the purposes of this subsection by an order made by the Secretary of State'.[200] In the intelligence agencies, it is an officer of the rank of General Duties 3 for all authorizations or notices or at General Duties 4 level.[201] This person was described by the ISC as 'a middle manager [who] reviews applications and records their reasons for approving or rejecting the application'.[202] More forensically, the Interception of Communications Commissioner describes the Designated Person as:

'… a person holding a prescribed office in the relevant public authority. The DP's function is to decide whether authority to acquire the communications data should be given … Except where it is unavoidable or for reasons of urgency or security, the DP should not be directly involved in the relevant legislation. The DP has to decide whether it is lawfully necessary and proportionate to acquire the communications data to which the application relates'[203]

74 The Designated Person considers the application and records his considerations at the time (or as soon as is reasonably practicable) in writing or electronically.[204] They must take account of any advice provided by the SPoC in assessing each application. The Designated Person must believe that it is necessary on any one of the **grounds set out in section 22(2)** to obtain communications data. These grounds are: the interests of national security, the purpose of preventing or detecting crime or of preventing disorder, the interests of the economic well-being of the United Kingdom, the interests of public safety, for the purpose of protecting public health, for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health or for any purpose which is specified for the purposes of this subsection by an order made by the Secretary of State.

75 Where the authorization has been obtained for the purposes of an investigation into criminal conduct by a member of a public authority problems can arise

198 *Ibid.,* para.4.42(2).

199 *Ibid.*

200 See Regulation of Investigatory Powers (Communications Data) Order 2010, SI 2010/480.

201 SI 2003/3172, Schs 1 and 2.

202 Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies* (Cm.8514, London, 2013), para.69.

203 *2013 Annual Report, of the Interception of Communications Commissioner* (2013–14 HC 1184) para.4.6.

204 Code of Practice, para.3.7. See further para.3.8.

in defining criminal conduct. This question was examined by the Investigatory Powers Tribunal in *C v Police and Secretary of State.*[205] Particular caution needs to be exercised where, on initial investigation, it is clear that no criminal conduct is being engaged in but the conduct may be of a disciplinary nature.

76 The Code of Practice next creates a further actor, the **'Senior Responsible Officer'** who is responsible for the integrity of the process within the public authority. Their terms of reference also include oversight of the reporting of errors to the Interception Commissioner and the identification of both the cause of errors and the implementation of remedial processes, and engagement with the Interception Commissioner inspections.[206] The Senior Responsible Officer must also ensure that the Designated Person and applicant makes available to the SPoC such information as the Senior Responsible Officer thinks necessary to ensure the integrity of any requirements for acquisition and compliance with Chapter II and with the Code of Practice.[207]

77 The ISC Report[208] attempts to set out the process for applying for, and authorizing, communications data by the intelligence services. There is no material difference in the procedure adopted by other public authorities entitled to seek authorization other than local authorities who must now also seek approval.

3. Authorisation

78 The application is made in writing or electronically or in exceptional cases orally.[209] Section 22(3) provides that the Designated Person may grant an authorization for persons with the same relevant public authority, provided, under section 22(5), it is proportionate to do so. DRIPA 2014 amends section 22(5) so as to provide for authorizations under section 22(3) or (3B) to relate to conduct outside of the United Kingdom and service of a notice under section 22(4) to a person outside the United Kingdom.[210] There is no statutory provision for the granting of authorizations or the giving of retention notices in urgent cases.[211] The postal or telecommunications operator must comply with any notice served under subsection (4)[212] unless it is not reasonably practicable to do so.[213] Where a postal or telecommunications operator does not discharge the duty, the Secretary of State can enforce it by way of civil proceedings for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.[214]

79 An authorization has **four mandatory requirements**. It must be in writing or in a manner that produces a record of the grant of authorization.[215] It must describe the conduct that is authorized and the communications data in rela-

205 IPT/03/32/H.

206 Code of Practice, para.3.31.

207 Code of Practice, para.3.32.

208 Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies* (Cm.8514, London, 2013), para.69.

209 Code of Practice, para.3.4 but note the requirement that a record of the application be made in writing or electronically as soon as possible.

210 DRIPA 2014, s.4(8)

211 Code of Practice, para.3.56.

212 RIPA 2000, s.22(6).

213 RIPA 2000, s.22(7).

214 RIPA 2000, s.22(8).

215 RIPA 2000, s.23(1)(a).

tion to which it is authorized.[216] It must specify which of the grounds set out in section 22(2) is relied upon[217] and specify the authorizing officer.[218] The Code of Practice also states that it must record the date and, where the case is urgent, the time the authorization is granted.[219] The Code of Practice also states that an authorization is not served upon the CSP. However, where the CSP, not unreasonably, wants an assurance that the conduct they are being asked to engage in is in fact lawful, details of the authorization may be disclosed or a copy of the authorization itself.[220]

80 Section 23(3) provides that a retention notice under section 22(4) shall not require the disclosure of data to any person other than the person giving the notice or such other person as may be specified.[221] However the notice must not specify or otherwise identify a person unless he or she holds an office, rank or position with the same relevant public authority as the person giving the notice.

81 Generally, the CSP should disclose the communications data in writing or electronically not later than the end of the period of **10 working days** from service, but a longer period of up to one month can be specified.[222]

82 Section 23 sets out the provisions in relation to the form and duration of authorizations issued under section 22(3) and notices issued under section 22 (4). An authorization or notice under section 23 ceases after one month.[223] Either an authorization or notice may be renewed.[224] There are provisions in relation to the cancellation of notices contained in section 23(8).[225]

83 The Secretary of State must ensure that arrangements are in place relating to the costs incurred with complying with notices under section 22(4).[226] The Code of Practice states that there is 'significant public funding' available to CSPs 'to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' requests for the acquisition and disclosure of communications data'.[227]

84 The Protection of Freedoms Act 2012 amends section 23 for local authorities and provides that the authorization or notice will not take effect until such time (if any) the relevant judicial authority has made an order approving the grant of the authorization or giving or renewal of the notice.[228] This reform reflects a concern that local authorities were applying these powers in trivial matters. Their regulation is beyond the scope of this paper.

4. Data Retention and Investigatory Powers Act 2014

85 DRIPA 2014 was introduced as emergency legislation in the aftermath of the decision of the Court of Justice of the European Union (CJEU) in *Digital Rights*

216 RIPA 2000, s.23(1)(b).
217 RIPA 2000, s.23(1)(c).
218 RIPA 2000, s.23(1)(d).
219 Code of Practice, para.3.28. For further requirements see para.3.37.
220 Code of Practice, para.3.27.
221 RIPA 2000, s.23(3).
222 Code of Practice, para.3.41.
223 RIPA 2000, s.23(4)(a).
224 RIPA 2000, s.23(5).
225 RIPA 2000, s.23(8).
226 RIPA 2000, s.24(1).
227 Code of Practice, para.4.3.
228 RIPA 2000, s.23A(2) as amended by s.37 of the Protection of Freedoms Act 2012.

Ireland Limited v Minister for Communications[229] which declared as invalid the Data Retention Directive. In reality, the opportunity was taken for a variety of other changes. The legislation is subject to a sunset clause and expires on 31 December 2016,[230] by which time an independent review is required under section 7. The review has been undertaken by David Anderson.[231] As previously noted, a Code of Practice has been issued in 2015.

86 The first two sections of DRIPA deal with retention of relevant communications data. Section 1 creates the 'retention notice' which can only be given if it is necessary and proportionate and meets one or more of the purposes falling within s 22(2).[232] Service of a retention notice on a public communications provider requires it to retain 'relevant communications data'. Relevant communications data are defined as the kind mentioned in the Schedule to the **Data Retention (EC Directive) Regulations 2009**[233] and include communications data relating to unsuccessful call attempts that in the case of telephony data, is stored in the United Kingdom and in the case of internet data, logged here. It does not include data relating to unconnected calls or data revealing the content of a communication.[234] However the **legality** of these Regulations is now **questionable** in light of the judgment of the CJEU in the *Digital Rights Ireland* case.

87 A retention notice may relate to a particular operator or any description of operators, require retention of all data or any description of data, specify the period or periods for which it is to be retained, contain other requirements or restrictions in relation to the retention of data, make different provision for different purposes and relate to data whether or not in existence at the time of the giving or coming into force of the notice.[235] These are vague and pervasive provisions, some of which can be traced back to the Communications Data Bill 2012. The Intelligence Services Committee[236] that concluded that whilst the Bill was 'deliberately broad to permit future-proofing of the legislation against technological change and not to reveal gaps in operational capability', the lack of specificity was 'causing considerable concern' to the public,[237] and so it recommended 'more thought is given to the level of detail that is included in the Bill'.[238]

229 C-293/12, 8 April 2014. See further Kühling, J., and Heitzer, S., 'Returning through the national back door? The future of data retention after the ECJ judgment on Directive 2006/24 in the UK and elsewhere' (2015) 40 *European Law Review* 263. The need to safeguard further has now been emphasised by the later judgment of the European Court of Justice in *Schrems v Data Protection Ireland*, Case C 362/14, 6 October 2015. Routine transfers of data by Facebook from Ireland to the USA under the aegis of the Safe Harbour Privacy Principles, which were approved by the European Commission (2000/520/EC) as fully meeting the requirements of the Data Retention Directive, failed to meet EU data protection standards because of the threat of 'indiscriminate surveillance … on a large scale' (para.31).

230 DRIPA 2014, s.8(3).

231 See Anderson, D., *A Question of Trust – Report of the Investigatory Powers Review* (Home Office, London, 2015).

232 DRIPA 2014, s.1(1).

233 SI 2009/859.

234 DRIPA 2014, s.2(2)

235 DRIPA 2014, s.1(2).

236 The Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies* (Cm 8514, London, 2013).

237 *Ibid.,* para.51.

238 *Ibid.,* para.79.

88 There is provision for the making of Regulations under section 2. The Data Retention Regulations 2014[239] include provision about the requirements before giving a retention notice, the maximum period for which data can be retained under a notice, the content, giving, coming into force, review, variation or revocation of a retention notice, integrity, security or protection of, access to, or the disclosure or destruction of, data retained under section 1, enforcement and auditing of the compliance with the requirements of section 1 and a Code of Practice.[240] The **maximum period** that data can be retained must not exceed **12 months**. Disclosure of communications data retained is restricted to the circumstances under which disclosure can be made under Part 1, Chapter 2, a court order or other judicial authorization or warrant or as provided for by the Regulations.[241]

89 This scheme is problematic. The first problem involves errors and excess data. There are two types of error: recordable (an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly)[242] and reportable (communications data are acquired or disclosed wrongly). In the case of the former an investigation must be undertaken[243] and record maintained by the public authority. In the case of the latter, a report must be made to the Commissioner[244] within five working days of discovery.[245] In 2013 there were 970 communications data errors which were reported to the Office of the Interception of Communications Commissioner. Almost half were caused by data being requested on the incorrect communications address.[246]

5. Challenges

90 The **acquisition and disclosure of communications data** have been amongst the most controversial aspects of the regulatory regime introduced by RIPA 2000. Aside from the legal battles over data retention, public disquiet has been generally fed by the revelations of former National Security Agency systems administrator Edward Snowden.[247] Mass interception is taking place, though the government claims that only limited messages are in fact monitored. This issue is being challenged in *Big Brother Watch and others v The United Kingdom*.[248]

91 Other significant controversies include the **extent** of what is counted as 'communications data', the generous interpretation of which caused the rejection of the draft Communications Data Bill 2012.[249] But, as shall be discussed in the conclusion, the government now proposes in part to revive some of the Bill's ideas to make available to the intelligence agencies web traffic data and data from a wider range of modes of communication. Another issue of coverage

239 SI 2014/2042.

240 DRIPA 2014, s.1(4).

241 DRIPA 2014, s.1(6). No further grounds have been specified.

242 Code of Practice, para.6.14.

243 *Ibid*., para.6.17.

244 Code of Practice, para.6.13.

245 Code of Practice, para.6.17.

246 *2013 Annual Report, of the Interception of Communications Commissioner* (2013–14 HC 1184) Points of Note, p. 38.

247 See Greenwald, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books, New York, 2014).

248 [2014] ECHR 93.

249 Cm.8359, London, 2012.

arose from the revelation in 2015 that bulk communications data collection by the intelligence agencies had long been authorised under the power for the Secretary of State to issue directions to Communications Service Providers under section 94 of the Telecommunications Act 1984. No form of oversight (other than judicial review) applies to this power.

92 Finally, there remain objections to the refusal to recognize clear exceptions for claims to privilege. In *News Group Newspapers v Commissioner of Police for the Metropolis*,[250] the Investigatory Powers Tribunal ('IPT') found that the 2007 version of the Code of Practice did not sufficiently protect **journalistic communications** when the purpose of the authorisation was to identify sources. However, the IPT also noted that a revised Code of Practice made in 2015 now requires that an application for communications data by a police force or law enforcement agency which is designed to identify a journalist's source should not be made under section 22 of RIPA but should be made under section 9 of the Police and Criminal Evidence Act 1984 ('PACE') which requires judicial authorisation.[251] An **exception** applies where there is believed to be an **immediate threat of loss of life** and that obtaining the data would dissipate the threat, in which case section 22 may be used, provided that such authorisations are notified to the Interception of Communications Commissioner as soon as reasonably practicable. However, the 2015 version has yet to make inroads into police practices with regard to journalists[252] and in any event makes no formal concession to the claims of **medical doctors**, **lawyers**, or **Members of Parliament** and asserts instead that 'Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.'[253]

IV. Surveillance

1. Scope and meaning

93 Like other forms of covert intelligence-gathering, state surveillance in the United Kingdom has **historically** been conducted **without any legislative structure**. However, there have been growing pressures for greater legal protection based on the positive desire to protect liberal concepts of autonomy but also because of negative perceptions about the dangers of surveillance[254] in a society which is seemingly 'achieving „the disappearance of disappearance"'.[255] The evolution of a statutory framework is also correlated to the influence of jurisprudence triggered by the ECHR, much of it relating to privacy and property interests.[256]

250 [2015] UKIPTrib 14 176-H.

251 Paras.3.78 to 3.84.

252 Interception of Communications Commissioner's Office, *Inquiry into the use of Chapter 2 of Part I of the Regulation of Investigatory Powers Act (RIPA) to Identify Journalistic Sources* (London, 2015). The report bemoans a lack of guidance in the RIPA Code on article 10 and also suggests that authorisations should be handled by judges.

253 *Ibid*., para.3.72.

254 See *Report of the Committee on Privacy* (Cmnd.5012, London, 1972); Information Commissioner, *A Report on the Surveillance Society* (Wilmslow, 2006); House of Commons Home Affairs Committee, *A Surveillance Society?* (2007–08 HC 58) and *Government Reply* (Cm.7449, 2008).

255 Haggerty, K.D., and Ericson, R.V., 'The surveillant assemblage' (2000) 51 *British Journal of Sociology* 605, 619. See further Lyon, D., *Surveillance Society* (Open University, Buckingham, 2001).

256 *Golder v UK*, App. no.4451/70,, Ser. A. vol.18, (1975); *Silver v UK*, App. no.5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 71361/75, Ser.A. vol.61 (1983); *Malone v UK*, App.

Another influence has been, exceptionally, the impact of scandalous revelations about excessive surveillance techniques. These have included undercover squads which infiltrated marginal groups of protest groups.[257] Another example concerns the flooding of residential areas with unmarked and unannounced surveillance cameras.[258]

94 The statutory response has primarily involved the RIPA 2000, Part II, which represented at the time of enactment a bold and comprehensive landmark attempt to control state surveillance[259] but which is now viewed as outdated and inadequate.[260] Under the legislation, surveillance includes (but is not limited to) **monitoring, observing or listening to persons**, their **movements**, their **conversations** or their other **activities** or **communications**.[261] It extends to the recording of such activity[262] and the use of a surveillance device (defined as 'any apparatus designed or adapted for use in surveillance').[263] However, in *Re A complaint of surveillance,*[264] the IPT held that 'the core activity of „surveillance" itself is not defined in s.26, nor is it defined in s.48 … s 48(2) refers to „surveillance", but does not define it'.[265] Nevertheless, it is possible to distil a number of elements from sections 26 and 48 that assist in understanding the definition. First, it must involve under section 48(2) the surveillance of persons, not property;[266] this seems a narrow interpretation and may be inconsistent with Strasbourg jurisprudence.[267] Second, it can involve various means, not all technological but some of ancient origins such as human agents. Third, it is intended by those carrying out the surveillance that the **subject should be unaware of the surveillance** and have **no chance to engage with the surveillance operator**. It follows that perhaps the most common forms of 'surveillance', overt CCTV or vehicle number recognition devices, are generally not covered by RIPA

no.8691/79, Ser. A. vol. 82, (1984); *Halford v UK*, App. no.20605/92, 1997-III; *Govell v United Kingdom*, App. no.27237/95, 14 January 1998; *Khan v UK*, App. no.35394/97, 2000-V; *PG and JH v UK*, App. no.44787/98, 2001-IX; *Armstrong v UK*, App. no.48521/99, 16 July 2002; *Perry v UK*, App. no.63737/00, 2003-IX; *Peck v United Kingdom* App. no.44647/98, 28 January 2003; *Wood v UK*, App. no.23414/02, 16 November 2004; *Gillan and Quinton v UK*, App. no.4158/05, 12 January 2010.

257 See Bonino, S., and Kaoullas, L.G., 'Preventing Political Violence in Britain: An Evaluation of over Forty Years of Undercover Policing of Political Groups Involved in Protest' (2015) *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2015.1059102.

258 See Walker, C., 'Championing local surveillance in counter-terrorism' in Davis, F., McGarrity, N., and Williams, G., *Surveillance, Counter-Terrorism and Comparative Constitutionalism* (Routledge, Abingdon 2014).

259 See Ferguson, G., and Wadham, J., 'Privacy and surveillance' [2003] *European Human Rights Law Review* Special Issue 101.

260 Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework* (2014–14 HC 1075); Anderson, D., *A Question of Trust – Report of the Investigatory Powers Review* (Home Office, London, 2015).

261 RIPA 2000, s.48(2)(a).

262 RIPA 2000, s.48(2)(b).

263 RIPA 2000, s.48(1), (2).

264 IPT/A1/2013.

265 *Ibid*., para.3.

266 Compare *Hoekstra and others v Her Majesty's Advocate* [2002] ScotHC 343.

267 See *Niemietz v Germany*, App. no.13170/88, Ser. A 251-B (1993).

2000,[268] though are subject to alternative regulation.[269] The position is more uncertain for online surveillance.[270] Fourth, recording the subject, even if done covertly, is not of determinative importance; it is only relevant if it takes place during activity that amounts to surveillance.[271]

'Surveillance' also extends to the interception of communications in the course of their transmission subject to the strict requirement that either the sender or recipient consents to the interception[272] and there is no warrant issued in connection with the interception[273] It excludes any conduct of a covert human intelligence source ('CHIS').[274] It also excludes trespass to, and interference with, property or wireless telegraphy unless authorized under section 5 of the ISA 1994 or Part III of the Police Act 1997.[275] **95**

Section 26 sets out matters common to both forms of surveillance. The surveillance must be carried out **covertly** and involve the **acquisition of private information**. Surveillance is carried out 'covertly' if 'it is carried out in a manner that is calculated to ensure that persons that are subject to the surveillance are unaware that it is or may be taking place'.[276] This formula may create difficulties. On the one hand, the intention of the relevant officers falls to be examined; on the other hand, the issue may be whether the target was subjectively aware or suspected that surveillance was taking place in fact. The latter was the approach preferred by the Court of Appeal in *R v Rosenberg*,[277] although the former is probably what Parliament intended. **96**

'Private information' is an express element of directed surveillance,[278] but it is probably also an element of intrusive surveillance. Private information in relation to a person includes any information relating to his or her private or family life.[279] The Code of Practice on Covert Surveillance and Property Interference helpfully makes it clear that even in a public place an expectation of privacy may exist, particularly 'where a record is being made by a public authority of that person's activities for future consideration or analysis'.[280] Two Scottish cases have further deliberated upon what amounts to 'private information'. In *Henderson and Marnoch v Her Majesty's Advocate*[281], the Scottish **97**

268 See McKay, S.,*Covert Policing: Law and Practice*, (2nd ed, Oxford University Press, Oxford, 2015) para.5.181.

269 See Protection of Freedoms Act 2012, Pt.II; Home Office, *Surveillance Camera Code of Practice* (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf, 2013); Information Commisssioner, *In the picture: A data protection code of practice for surveillance cameras and personal information* (https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf, 2015).

270 See *Annual Report of the Chief Surveillance Commissioner for 2012–2013* (2012–13 HC 577) para.5.7; O'Floinn, M., and Ormerod, D., 'Social networking sites, RIPA and criminal investigations' [2011] *Criminal Law Review* 766.

271 IPT/A1/2013, para.32.

272 RIPA 2000, s.48(4)(a).

273 RIPA 2000, s.48(4)(b).

274 RIPA 2000, s.48(3).

275 RIPA 2000, s.48(3)(c)(i)–(ii).

276 RIPA 2000, s.26(9)(a).

277 [2006] EWCA Crim 6.

278 RIPA 2000, s.26(2)(b).

279 RIPA 2000, s.26(10).

280 (2014) para.2.5.

281 2005 HCJAC 47.

Appeal Court held that recordings of threats of violence and extortion that took place without appropriate authorization being in place 'can hardly be described as comprising any form of „private information"'.[282] In *Kinloch v Her Majesty's Advocate*[283], the UK Supreme Court approved an earlier decision of the Scottish Appeal Court in *Gilchrist v Her Majesty's Advocate*[284] in which Lord Macfadyen stated that where the activity took place 'in a public place … observed by anyone who happened to be in the vicinity, whatever the reason for their presence might be … [it] did not involve the obtaining of private information'.[285]

98 For regulatory purposes, section 26 goes on to create two categories of surveillance – **'directed'** and **'intrusive'**, but where surveillance involves trespass to or interference with property or wireless telegraphy, then Part III of the Police Act 1997 or the ISA 1994 apply in priority.[286]

2. 'Directed surveillance'

99 As for **'directed' surveillance**, 'surveillance is directed … if it is covert but not intrusive' and meets three criteria. **First**, it is carried out for the purposes of a specific investigation.[287] **Secondly** it is carried out in such a manner as is likely to result in the obtaining of private information about a person whether specifically identified as part of the specific investigation or operation or not.[288] **Thirdly**, it is carried out other than by way of an immediate response to events or circumstances that is such that it would be reasonably impracticable to obtain authority to engage in surveillance activity. Surveillance is 'covert' under section 26(9) if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware of it.[289]

100 Authorisation of 'directed' surveillance is by a 'designated person' within any of the authorities set out in section 28 and Schedule 1 of RIPA 2000 (for instance, a police inspector or General Duties 3 level intelligence agency officer).[290] They may be subject to restrictions on the authorizations they may grant and the circumstances in which or the purposes for which they may grant authorizations.[291] Authorizations for directed surveillance are governed by section 29. Designated persons can only grant authorizations if they believe there are grounds to do so[292] and the proposed surveillance to be authorized is proportionate.[293]

101 The **grounds** upon which an authorization may be granted under section 28 (3) are any of the following: the interests of national security, for the purpose of

282 *Ibid.,* para.10.
283 [2012] UKSC 62.
284 2005 (1) JC 34.
285 *Ibid*., para.21.
286 See RIPA 2000, s.48(3)
287 RIPA 2000, s.26(2)(a).,
288 RIPA 2000, s.26(2)(b).
289 RIPA 2000, s.26(9)(a).
290 See Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000, SI 2000/2417 as amended by SI 2002/1298SI 2003/3173, SI 2005/1084, SI 2006/594. Local authorities are also able to authorise directed surveillance, subject to judicial approval under s.32A.
291 RIPA 2000, s.30(3); Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521).
292 RIPA 2000, s.28(2)(a); the grounds are set out in s.28(3)(a)–(g).
293 RIPA 2000, s.28(2)(b). See further *Report of the Chief Surveillance Commissioner for 2000–2001* (Cm.5360, London, 2002) paras.4.13, 4.14.

preventing or detecting crime or of preventing disorder, the interests of the economic well-being of the United Kingdom, the interests of public safety, for the purpose of protecting public health, for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, or for any purpose other than the above which is specified by order. Applications for directed surveillance in national security cases are, in general, the province of the **Security Service**. The only exceptions are where the operations are carried out by police units with a formal counter-terrorism role or where the Security Service has agreed that another public authority can carry out the surveillance on its behalf.[294] Her Majesty's armed forces can undertake surveillance in connection with the military threat to national security, in support of the Security Service and the Police Service of Northern Ireland.[295]

102 The conduct that is authorized by a directed surveillance authorization is the directed surveillance as specified in the authorization, provided it is carried out in the circumstances described in the authorization and for the purposes of the investigation or operation specified or described in the authorization.[296]

103 The Code of Practice identifies **ten matters** that need **to be covered** in an application and it is against this list that authorizations will be checked by authorizing officers, reviewed by the Office for the Surveillance Commissioners on an inspection, or considered in legal proceedings. The list comprises: the reasons why the application is necessary and the grounds upon which it is based, the nature of the surveillance engaged in, the identities of the targets, a summary of the intelligence case, the information it is hoped will be acquired as a result of the deployment, an assessment of collateral intrusion and why it is justified in the circumstances, any confidential information at risk of being acquired, an assessment of the proportionality of the proposed operation, the level of authority required and the record of decision and its date and time.[297] The Chief Surveillance Commissioner has emphasized the need for precision in applications for authorizations.[298]

104 Authorization can be **granted or renewed** orally in an urgent case or must otherwise be in writing.[299] In cases where authorization is given in writing, it lasts for three months,[300] or, in the case of an authorization granted by an intelligence agency, for six months.[301] An urgent application may be authorized for up to 72 hours.[302]

A directed surveillance authorization may be renewed.[303] An authorization must be cancelled if the grounds upon which it was granted are no longer satisfied.[304] Once cancelled, surveillance should cease immediately.

105 Directed surveillance by law enforcement stood at approximately 20,000 cases in 2006–07 and by other public authorities was at its height in 2006–07

294 Code of Practice, fn 30.
295 Code of Practice, fn 31.
296 RIPA 2000, s.28(4).
297 Code of Practice, para.5.8.
298 *Report of the Chief Surveillance Officer, 2003–2004* (2003–04 HC 668) pp. 11–12.
299 RIPA 2000, ss.34(1)(a), 43(1). See also SI 2003/3171, SI 2005/1084, SI 2006/594, SI 2006/1874.
300 RIPA 2000, s.43(3)(c). See further s.43(9) for timings.
301 RIPA 2000, s.44(5).
302 RIPA 2000, s.43(3)(a)(i).
303 RIPA 2000, ss.43(4), 44(7).
304 RIPA 2000, s.45(1)(a).

at over 12,000 reflecting the climate of counter terrorism after the 7/7 attacks. Directed surveillance by law enforcement stood at around 10,000 for 2012–13 and 2013–14 and for public authorities at around 4,000.[305]

3. 'Intrusive surveillance'

106 Moving now to consider 'intrusive' surveillance, surveillance is **'intrusive'** if carried out in relation to anything taking place on any **residential premises** or in any **private vehicle**[306] and involves the presence of an individual on the premises or in the **vehicle** or is carried out by means of a surveillance device.[307] Any surveillance by way of a device adapted for the purpose of providing information about the location of a vehicle or which amounts to an interception of a communication[308] as falls within section 48(4) is not 'intrusive' surveillance; in those circumstances, the Code of Practice provides guidance that either forms of conduct may amount to directed surveillance.[309] In the last three years, authorisation for the security agencies to enter property and plant surveillance devices was granted in 2447 cases. Of these 1344 involved suspected drugs trafficking, 235 robbery, 152 kidnap/extortion, 148 murder, 106 money laundering and 17 terrorism.[310]

107 Given the more serious potential interference with privacy, authorisation under section 32 requires either the assent of a senior authorizing officer (such as the Chief Constable of any police force)[311] or the Secretary of State (for the security agencies). The matrix for authorizing intrusive surveillance further creates for the police a system of independent review. Thus, any authorisation for the police and other designated public authorities[312] must be also notified under section 35 to a Surveillance Commissioner (see below) who must also give approval for the authorisation to take effect under section 36. However, the authorization regime differs in cases of intrusive surveillance by the intelligence agencies, the Ministry of Defence and Her Majesty's forces. Applications for authorization are made to the Secretary of State and do not need the approval of the Surveillance Commissioner.

108 The **grounds** upon which authority may be granted under section 32(3) are: in the interests of national security; for the purpose of preventing or detecting serious crime; or in the interests of the economic well-being of the United Kingdom. However, the latter ground is omitted in relation to applications by the Ministry of Defence and Her Majesty's forces.[313] Furthermore, applications by the SIS or GCHQ in regard to serious crime must show that they are acting in support of a law enforcement agency rather than independently.[314] The functions of the Security Service are extended by section 42. Provided it is acting within powers exercisable by SIS or GCHQ other than anything done in support

305 *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013–2014* (2013–14 HC 343) paras.4.7–4.8.

306 RIPA 2000, s.26(3)(a).

307 RIPA 2000, s.26(3)(b).

308 RIPA 2000, s.26(4).

309 Code of Practice, paras.2.8, 2.20.

310 *Ibid.,* Appendix B.

311 See especially Ministry of Defence Police Act 1987.

312 The provisions relating to designated public authorities are in RIPA 2000, s.41(4)–(6).

313 RIPA 2000, s.41(2).

314 RIPA 2000, s.42(3).

of the prevention and detection of serious crime,[315] it may act on either agency's behalf in relation to any application for a Part II authority (not limited to intrusive surveillance).[316] Proportionality and necessity must also be satisfied under section 32(2).

109 Where an intelligence agency is granted an authorization, it takes the form of a **Ministerial warrant**.[317] This warrant can combine an intrusive surveillance authorization and a warrant issued under the ISA 1994 (property interference), but the two legislative regimes must be considered and applied separately in the application before the Secretary of State.[318] There are special rules over and above those covered above in relation to authorities granted by or warrants issued to the intelligence agencies.[319] Only the Secretary of State can issue or renew a warrant containing an intrusive surveillance authorization.[320] If it is not renewed the warrant will cease to have effect at the end of the second working day following the day of issue (as opposed to the 72 hours in other cases).[321]

110 All applications must provide, as a minimum, the information listed in the Code of Practice, similar to directed surveillance.[322] An authorization may be granted or renewed orally in urgent cases[323] but otherwise must be granted in writing.[324]

111 If it is a combined application the separate provisions within RIPA must be considered as appropriate to those aspects of the application to which they relate.[325]

112 An authorization[326] that was granted or renewed on the basis that it was urgent will **cease to have effect after 72 hours**.[327] However, where the case is not urgent, for both directed and intrusive surveillance, the authority will cease to have effect after three months from the date it was granted or, if renewed, from the date of the latest renewal.[328] Different time periods apply to cases requiring Ministerial warrants involving the intelligence agencies. The first qualification, itself subject to qualification, is that the authorization may be renewed before it ceases to have effect by someone entitled to grant it.[329] The second qualification is that a warrant authorising the intelligence agencies can endure for a period of six months – twice as long as normal.[330] The same time periods apply to directed surveillance. Any authorization or renewal must be cancelled by the person who granted or renewed it (or a person entitled to act

315 RIPA 2000, s.42(5).
316 RIPA 2000, s.42(4).
317 RIPA 2000, s.42(1).
318 RIPA 2000, s.42(2).
319 RIPA 2000, s.43(10).
320 RIPA 2000, s.44(1), (2).
321 RIPA 2000, s.44(3).
322 Code of Practice, para.6.19.
323 RIPA 2000, s.43(1)(a); note that the person who grants or renews it must be entitled to do so in cases other than urgent cases, so as to ensure a senior level of oversight.
324 RIPA 2000, s.43(1)(b).
325 RIPA 2000, s.43(2).
326 The time of commencement of an authorisation or a renewal is specified in s.43(9).
327 RIPA 2000, s.43(3)(a).
328 RIPA 2000, s.43(3)(c).
329 RIPA 2000, s.43(4).
330 RIPA 2000, s.44(4)(a).

or that person's deputy)[331] if the requirements which were met when it was granted or renewed are no longer satisfied.[332]

113 Intelligence agencies must ensure that arrangements exist that ensure no information is held other than is necessary.[333] The Data Protection Act 1998 and Criminal Procedure and Investigations Act 1996 (regarding the retention of data for criminal processes) apply.[334] Material obtained through the deployment of directed or intrusive resources may be used in connection with other investigations.[335] However, in the case of trial issues, especially in criminal prosecutions where Closed Material Procedures do not apply,[336] a variety of mechanisms will tend to **exclude the usage of materials gathered** by **the intelligence agencies**.[337]

4. Challenges

114 The application of these measures to lawyers has proven troublesome. In *RE v UK*,[338] the police refused to give assurances that there would not be **covert surveillance** of consultations in the police station with a **lawyer** or an appropriate adult, the activity being treated as a form of directed surveillance. On judicial review, the Divisional Court directed that there be no covert surveillance of the legal consultations because of insufficient protection under the applicable regime, and the House of Lords agreed with the Divisional Court that although the provisions of RIPA could override, *inter alia*, legal professional privilege, the higher level of authority necessary for an intrusive surveillance warrant was required rather than the directed surveillance warrants that had hitherto been issued.[339] The ECtHR found a breach of article 8 in relation to the lawyer which must be subject to 'strengthened protections' because of the 'extremely high degree of intrusion' but no breach in relation to the appropriate adult where no enhanced standard of protection applied and adequate safeguards were in place.[340] Subsequently, under the RIPA (Extension of Authorisation Powers: Legal Consultations) Order 2010,[341] the Commissioner must consent to surveillance of lawyers. However, the ECtHR expressed itself as 'not satisfied that the provisions in Part II of RIPA and the Revised Code concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings may or must be erased or the material destroyed provide

331 RIPA 2000, s.45(2)(a)–(b); the list of such persons is set out in s.45(6).

332 RIPA 2000, s.45(1)(a)–(b).

333 Code of Practice, para.9.7.

334 Code of Practice, paras 9.3, 9.4 and 9.6.

335 Code of Practice, para.9.5.

336 See Walker, C., 'Terrorism prosecution in the United Kingdom: Lessons in the manipulation of criminalisation and due process' in Gross, O., and Ní Aoláin, F., *Guantanamo and Beyond: Exceptional Courts and Military Commissions in Comparative and Policy Perspective* (Cambridge University Press, Cambridge, 2013).

337 See McKay, S., *Covert Policing: Law and Practice*, (2nd ed, Oxford University Press, Oxford, 2014) chap. 9.

338 App. no.62498/11, 27 October 2015.

339 *Re C & Others* [2007] NIQB 101A; *Re McE* [2009] UKHL 15.

340 *Ibid.,* paras.131, 159, 167.

341 SI 2010/461

sufficient safeguards for the protection of the material obtained by covert surveillance.'[342]

V. Covert Human Intelligence Sources ('CHIS')

A limited commentary will be provided on CHIS since much of the legal catalogue is directed toward the use of their evidence in criminal courts (including issues of entrapment, anonymity and self-incrimination) or their treatment at criminal sentencing.[343] These contexts are of limited relevance to the intelligence agencies, though the value of CHIS to the agencies is unmistakable in activities such as disruption and preemption.[344] In his otherwise damning report in 2012 into the murder of Northern Irish solicitor, Patrick Finucane, Sir Desmond de Silva QC noted that 'intelligence gained from human agents is, clearly, a potent weapon for the State in countering terrorism',[345] but he recognised significant problems associated with a lack of a framework for their use. The activities of undercover squads of the Metropolitan Police Service have fully illustrated those problems even when it is the police officer who acts as the CHIS.[346] **115**

1. Scope

Section 26 applies to the use and conduct of CHIS. The definition is found in section 26(8) of RIPA. It is characteristically dense: **116**

'[A] person is a covert human intelligence source if

(a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);

(b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.'

The terms covert 'purpose' and covert nature of 'relationship', which includes use and acquisition of information are defined in subsection (9): **117**

'For the purposes of this section

(a) …

(b) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted

342 App. no.62498/11, 27 October 2015, para.141.

343 See *ibid*., chap 7.

344 See Phillips, D., Caless, B., and Bryant, R., 'Intelligence and its application to contemporary policing' (2007) 1(4) *Policing* 439; Moran, J., 'Evaluating Special Branch and the use of informant intelligence' (2010) 25(1) *Intelligence and National Security* 1.

345 de Silva, D., *The Report of the Patrick Finucane Review*, (2012–13 HC 802, 2012) paras.21–26.

346 Hyland, K., and Walker, C., 'Undercover policing and underwhelming laws' [2014] *Criminal Law Review* 555; Bonino, S., and Kaoullas, L.G., 'Preventing Political Violence in Britain: An evaluation of over forty years of undercover policing of political groups involved in protest' (2015) *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2015.1059102.

in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose; and

(c) a relationship is used covertly, and information obtained as mentioned in subsection (8)(c) is disclosed covertly, if and only if, it is used, or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.'

118 Subsection 9(a) requires the source to establish or maintain **'a personal or other relationship with a person'**. The ambit of establishing or maintaining the relationship is wide and includes any recruitment of a CHIS through inducements, or asking or assisting the person concerned to engage in the conduct of a CHIS. This broad and vague terminology also catches the CHIS in relation to the conduct in which he or she may subsequently engage. Equally and sensibly, it excludes members of the public who volunteer information to the police, through for example, a telephone hotline.[347]

119 The CHIS must covertly use the relationship to obtain information or provide access to any information to another person or covertly disclose information obtained through or as a consequence of the existence of the relationship. The term 'covertly' is defined separately for these purposes as relating to purpose and use. In short, both require that the relationship be conducted in a manner calculated to ensure that one of the parties to the relationship is 'unaware of the existence of the relationship or the use or disclosure in question'. There is an element of **subjectivity** here. The focus will be on how the authority and source conduct the relationship, not whether it is in fact conducted in a covert manner (in other words, the fact that one of the parties believes or discovers he or she is the subject of an undercover operation involving the use of a source does not negate the nature of the authorised use and conduct). Logically, it is unlikely that the 'authority' or the source will be 'one of the parties' unaware of the use or disclosure, so the only persons this provision will practically relate to are the target or targets of the investigation or those from whom the source acquires information.

120 There is another factor that broadens the definition of what may amount to 'use and conduct' and that is the clear and presumably intentional decision by those who drafted RIPA to use the considerably lower threshold of 'information' as opposed to 'private information' that is to be found in the definitions of directed and intrusive surveillance.[348] This is explained in the Code of Practice:

'[A]uthorisations for the use or conduct of a Covert Human Intelligence Source do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information.'[349]

347 Covert Human Intelligence Sources Code of Practice, para.2.14.

348 Code of Practice, para.2.11

349 Code of Practice, para.2.10

Defining a CHIS is further complicated by the terms 'establish' and 'maintain' in section 26(8). It is important to remember that relationships are established and maintained in many ways, not always with the consent of those involved. Previously, the emphasis was on 'tasking' defined in the former Code of Practice as 'the assignment given to the source by the persons defined at section 29(5)(a)' (persons with day-to-day responsibility for the source).[350] The Code of Practice, which has since been revised in 2010, has been criticized in the past for providing 'no guidance as to the **permissible limits of the activities of such individuals** … such advice barely merits the term „guidance"'.[351] In resolving the question of whether a CHIS is acting as such, the Code simply states 'determining the status of an individual or organisation is a matter of judgement by the public authority'.[352] It is interesting to note the context for this observation – the example given is that the source 'may be tasked with finding out purely factual information about the layout of commercial premises'.[353] This is problematic for at least two reasons. First, as noted above, the definition categorizes the nature of what a source may acquire as no more than 'information'; the determinative feature of this is that it is calculated that the target or third party is unaware of it. Secondly, a company may have privacy-based rights.[354] **121**

In *Allan v United Kingdom,*[355] the issues arising out of the deployment and use of what would have amounted to a CHIS during a murder investigation were considered. The government in *Allan* sought to rely on *Khan v The United Kingdom*[356] arguing there was no proper basis upon which it was possible to distinguish between a technical listening device (as was the case in *Khan*) and evidence admitted as a result of an informer wearing a recording device and that due to the seriousness of the offence it was in the public interest to admit the **informer's evidence**. The applicant drew the obvious distinction between his case and that of *Khan*, claiming recordings in their case were more invasive and protracted, that the evidence was inaccurate, and that the police informer was a resource to circumvent protections about police interrogations.[357] The ECtHR found that, whereas the use of recordings of voluntarily made statements obtained covertly did not violate Article 6, the use of the informant to circumvent Allan's **privilege against self-incrimination** and his **right to silence** did so. The Court found that Allan's right to silence had been sufficiently undermined to constitute an Article 6 violation on the basis that first the informant was acting as an agent of the state at the time the incriminating statement was made, and that secondly he had caused it to be made. With regard to the first of these considerations, a 'but for' test was appropriate to be applied whereby the question the court should ask is, whether the exchange between informer and suspect would have taken place in the same manner and form *but for* the authorities' intervention. The second consideration, whether the informant actually **122**

350 The former Code of Practice, para.4.26.

351 Starmer, K., et al, *Criminal Justice, Police Powers & Human Rights* (Blackstone Press, London, 2001) 68.

352 Code of Practice, para.4.29

353 *Ibid.,* para.4.29

354 *R v Broadcasting Standards Commission, ex parte British Broadcasting Corporation* [2000] 3 WLR 1327; 3 All ER 989.

355 *Allan v United Kingdom*, App. no.48539/99, 5 November 2002.

356 *The Times*, 23 May 2000.

357 See Police and Criminal Evidence Act 1984, Pt.IV.

caused the disclosure, appears to depend on an objective assessment of whether 'the conversation between him and the accused was the functional equivalent of an interrogation', as well as on the nature of the relationship. A distinction between *Khan* and *Allan* was made, statements in the latter being 'not spontaneous and unprompted … but … induced by the persistent questioning'[358] of the informer, who had been directed to channel conversations with Allan towards the murder. Analysing the relationship between Allan and the informer, the court found that although it was not 'special', Allan was subjected to 'psychological pressures'[359], which might negate the 'voluntariness' of what he said. Consequently, the use at trial of information gained in this way impinged on the defendant's right to a fair trial.

123 *Allan* was a decision on the application of Article 6, not the more obviously applicable Article 8, but the judgment is capable of importing lessons in that regard. The ECtHR placed considerable emphasis on the nature of the relationship the source shares with the target of the investigation both in terms of whether it is special but also risks offending the **protection against self-incrimination**. These are essential questions that need to be asked. If the source is an undercover officer, a close friend or indeed related or involved in a relationship with the target a need to authorize may arise, whereas if the relationship is more remote, it may not. Even if it is remote, then a critical part of the operational planning will be to ensure the dialogue the CHIS engages in with the target does not circumvent fairness as to questioning, particularly if it is envisaged this will form part of an evidential case against him. Amongst the critical considerations here will be whether the accused is in custody as well as the voluntary nature of any admissions made. These are to be **distinguished** from cases where a **listening device** installed in a police van picks up conversations between suspects post-charge, which are entirely voluntary.[360]

2. Authorisation[361]

124 There is no requirement for any relevant public authority to obtain authorization for the use and conduct of a CHIS.[362] However where no authorization has been obtained, the use and conduct may be deemed to have violated the ECHR, Article 8.

125 Authorization of sources is largely confined to section 29 of RIPA 2000. It can only be authorized where necessary[363] on one or more of the grounds found in subsection 3, which are the same for directed surveillance and include national security,[364] through most public authorities act on the ground of prevention and detection of crime.[365] The authorized conduct or use must be proportionate.[366]

358 *Allan v United Kingdom,* App. no.48539/99, 5 November 2002, para.52

359 *Ibid.*

360 See *Plunkett v R* [2013] EWCA Crim 261; *Khan, Mahmood and Kajla v R* [2013] EWCA 2230.

361 See generally, Code of Practice, Chapter 3. The authorisation regime under RIPA has been radically overhauled in respect of local authorities' use of CHIS under the Protection of Freedoms Act 2012 (omitted here).

362 RIPA 2000, s.80.

363 RIPA 2000, s.29(2)(a).

364 RIPA 2000, s.29(3)(a).

365 Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521 (as amended).

366 RIPA 2000, s.29(2)(b).

The nature of the conduct is specified in subsection 4 and includes any activities involving the conduct of a source[367] or the use specified or described in the authorization[368] and carried out for the purposes of or in connection with the operation or investigation to which the authorization relates.[369] Subsection 5 imposes various duties. There must be at all times a person within the authorizing organization who will have on its behalf **day-to-day responsibility** for dealing with the source and his or her security and welfare.[370] There must also be a different person within the organization who will have oversight of the use made of the source.[371] Either of these persons or another must have responsibility for **maintaining records** of the use made of the source.[372] The records should be held centrally and should be retained for a period of not less than three years following the ending of the authorization period.[373]

126 The organizations entitled to authorize the use and conduct of CHIS are listed in Schedule 1 of RIPA (including the intelligence agencies). The persons entitled to grant authorizations ('Designated Persons') are given effect by a Ministerial Order.[374] Designated Persons must not grant an authorization for the use and conduct of a source except on an application being made by a member of their organization.[375] There are provisions in section 31 for limiting the making of orders under section 30 insofar as they relate to conduct by public authorities under RIPA in Northern Ireland. Where an authorisation combines an authorisation under section 28 or 29 and an authorisation by the Secretary of State for the carrying out of intrusive surveillance, the Secretary of State is the person designated.[376]

127 Section 43(2) enables a single authorization to combine two or more authorizations under Part II of RIPA but the provisions of the Act that apply in respect of each authorization must be considered separately. Where an application combines the proposed use of more than one covert policing resource that requires a hierarchy of authorization, it must be the senior authorizing authority that authorizes. Thus the Code of Practice makes clear that 'where an authorisation for the use or conduct of a covert human intelligence source is combined with a Secretary of State authorisation for intrusive surveillance, the combined authorisation must be issued by the Secretary of State'.[377]

128 Authorization can be granted or renewed orally in an urgent case but must otherwise be in writing.[378] An urgent application may be authorized for up to

367 The person specified in the authorization, RIPA 2000, s.29(4)(b).

368 RIPA 2000, s.29(4)(a).

369 RIPA 2000, s.29(4)(c).

370 RIPA 2000, s.29(5)(a).

371 RIPA 2000, s.29(5)(b).

372 RIPA 2000, s.29(5). See Regulation of Investigatory Powers (Source Records) Regulations 2000, SI 2000/2725.

373 Code of Practice, para.7.1. See also Rose, C.,*Ratcliffe-on-Soar Power Station Protest Inquiry into Disclosure* (CPS, London, 2011); *An Informer v A Chief Constable* [2012] EWCA Civ 197, paras 19–20

374 Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, SI 2010/521 (as amended).

375 RIPA 2000, s.33(1) and (2).

376 RIPA 2000, s.30(2).

377 Code of Practice, para.3.25 (n. 17)

378 RIPA 2000, s.43(1). See further s.34(1)(a).

72 hours[379] before it is required to be renewed. In cases where authorization is given in writing, it lasts for 12 months.[380]

129 Following reviews of the Mark Kennedy case,[381] special rules were introduced on authorisation in cases where the deployment is 'long term' or involves a 'relevant source' (an officer) under the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013.[382] However, the Order excludes the intelligence agencies.[383]

130 There are a number of tricky circumstances that arise, including the potential or actual acquisition of confidential and privileged material, and the treatment of vulnerable or **juvenile sources**. These will not be taken up here. Other complications can arise where the use of a CHIS engages other surveillance techniques, such as the collection of intercept data.[384] These issues were considered in *R v McDonald and others*.[385] The case involved the prosecution of three Real IRA terrorists whose telephone conversations between undercover Security Service officers and agents were used as evidence in the case by the prosecution. These ought to have fallen outside the Part I RIPA 2000 regime because the CHIS consented. The practical effect of the statute and Code of Practice is to require the covert human intelligence sources authorization to provide for the surveillance of telephone calls recorded between the source and the target within its terms. In *McDonald* this was not done at the outset though was subsequently. The trial judge, Astill J ruled the evidence admissible. JUSTICE has repeatedly suggested that source-borne eavesdropping or listening devices or 'participant monitoring' are incompatible with the ECHR[386] relying on the Canadian authority of *Duarte*.[387] The issue has yet to be the subject of challenge.

3. Participation in criminality

131 The regulatory framework in section 26 of RIPA does not expressly permit a CHIS to participate in criminality. However, section 27 makes lawful 'for all purposes'[388] conduct if an authorization under Part II of RIPA confers an entitlement on the part of a source to engage in such conduct providing he or she does not exceed the terms of such authority. In *Re McE,*[389] Lord Hope held that 'the whole point of the system of authorisation that [RIPA] lays down is to interfere

379 RIPA 2000, s.43(3)(a)(i).

380 RIPA 2000, s.43(3)(b).

381 Her Majesty's Inspector of Constabulary (HMIC)*, A Review of National Police Units which provide intelligence on criminality associated with protest* (Home Office, London, 2012); Independent Police Complaints Commission, *Ratcliffe-on-Soar Power Station (Operation Aeroscope) Disclosure Nottinghamshire Police* (London, 2012); Rose, C., *Ratcliffe-on-Soar Power Station Protest: Inquiry into Disclosure* (CPS, London, 2011); Home Affairs Select Committee, *Undercover Policing: Interim Report* (2012–13, HC 837). Also note Ellison, M., *The Stephen Lawrence Independent Review: Possible corruption and the role of undercover policing in the Stephen Lawrence case,* (2013–14 HC 1038).

382 SI 2013/2788.

383 SI 2013/2788, article 2.

384 Code of Practice, para.3.25.

385 (Woolwich Crown Court, 23 April 2002); [2005] EWCA Crim 1945, [2005] EWCA Crim 1970. See also *R v Hardy* (Court of Appeal, 31 October 2002).

386 *Under Surveillance*, (London, 1998).

387 [1990] 1 SCR 30.

388 RIPA 2000, s.27(1).

389 [2009] 1 AC 908

with fundamental rights and to render this invasion of a person's private life lawful'.[390] The former Code of Practice on Covert Human Intelligence Sources stated that a use and conduct authorization may 'in a very limited range of circumstances' render unlawful conduct that would otherwise be criminal lawful.[391] It now states more circumspectly, 'neither Part II of the 2000 Act nor this code of practice is intended to affect the existing practices and procedures surrounding criminal participation of CHIS'.[392]

The High Court considered the **limits of the conduct** which a CHIS may be authorised to engage in the light of activities by undercover police officer Mark Kennedy and others.[393] Kennedy infiltrated environmental protest groups for the National Public Order Intelligence Unit of the Association of Chief Police Officers (since rebranded along with the National Extremism Tactical Co-ordination Unit as the National Domestic Extremism and Disorder Intelligence Unit and configured as part of the Metropolitan Police Service Counter Terrorism Command).[394] The Court held that conduct that amounts to an interference with the fundamental right not to be subjected to degrading treatment cannot be authorised. The same point must also extend to the right to life. Interference with the right to privacy is capable of being authorized, subject to **necessity** and **proportionality**. This includes, in principle, a CHIS engaging in a sexual or other intimate relationship with another person in order to gain access to information. Mr Justice Tugendhat expressed the view that section 27 *only* applies to unlawful conduct but accepted the provision gave rise to 'difficult issues'.[395] However, it is not clear that section 27 is limited to unlawful conduct. As the Investigatory Powers Tribunal observed in *C v Police and Secretary of State,*[396] 'surveillance by public authorities is not of itself unlawful at common law, nor does it necessarily engage Article 8'.[397] If the intention behind the provision was to make the activities lawful solely for the purposes of Article 8(2), then it is difficult to understand the implications of the decision in *R v GS and eight others*,[398] a case that explored the susceptibility of the Office of Surveillance Commissioners to cross-examination. The Court of Appeal ruled that a Com- **132**

390 *Re McE* [2009] UKHL 15, para.61

391 Code of Practice, para.2.10

392 Code of Practice, para.1.9. See also consideration of the technique of undercover officers assuming the identities of dead babies: Creedon, M., *Operation Herne. Part One Use of Covert Identities* (MPS, London, 2013).

393 *AJK and others v Commissioner of the Police for the Metropolis* [2013] EWHC 32 (QB), paras.156–164. Further procedural issues were considered in the Court of Appeal ([2013] EWCA Civ 1342) and in DIL and others v *Commissioner of the Police for the Metropolis* [2014] EWHC 2184 (QB). The Metropolitan Police later settled the case and acknowledged that the relationships were 'a violation of the women's human rights, an abuse of police power and caused significant trauma.' (http://news.met.police.uk/news/claimants-in-civil-cases-receive-mps-apology-138574, 20 November 2015).

394 https://www.mi5.gov.uk/home/about-us/what-we-do/the-threats/terrorism/domestic-extremism.html.

395 [2013] EWHC 32 (QB), para.167.

396 IPT/03/32/H.

397 *Ibid*., para.42

398 [2005] EWCA Crim 887.

missioner could not be called to test lawfulness by virtue of section 27(1) and that it clearly applied to criminal proceedings.[399]

133 At its simplest, where a relevant public authority wishes to use an individual to obtain or disclose information through establishing or maintaining a personal relationship with the suspect, the nature of which is covert (and so conducted in a manner that is calculated to ensure that the suspect is unaware of the purpose of the relationship or the disclosure of information obtained as a consequence of the relationship),[400] then there will be a need to authorize the individual as a CHIS, whether or not, if the public authority wishes to have the protection of section 27.[401] Where the position is less clear, consideration should be given to the factors identified in *Allan v United Kingdom*[402] and a decision taken to authorize or not.

4. Civil liability

134 Civil liability arising out of the use and conduct of sources can arise in contract, tort and under the HRA 1998. The litigation against the Metropolitan Police Service's undercover officers, noted above, has been the most prominent example. Fewer cases have arisen against the intelligence agencies,[403] so this matter will be left to the discussion of liabilities later in this paper.

5. Challenges

135 The use of informants has remained largely unregulated by law until recent times and was poorly regulated by internal practice rules. Sir Desmond de Silva QC's report into the murder of Northern Irish solicitor Patrick Finucane, allegedly through the involvement of Loyalist terrorist agents set up by the security agencies, made clear that 'there was a wilful and abject failure by successive governments to provide the clear policy and legal framework necessary for agent-handling operations to take place effectively and within the law.'[404] Though **police handling** of CHIS has become **more tightly controlled** following successive RIPA reforms, most **do not apply to intelligence agencies** whose scandals have been more successfully suppressed.

VI. Encryption

136 The provisions relating to the investigation of data protected by encryption are found in Part III of RIPA 2000 and Code of Practice on the Investigation of Protected Electronic Information.

---

399 See Hopkins, A., 'Testing lawfulness: the authorisation of interceptions and covert surveillance under the Regulation of Investigatory Powers Act 2000' [2005] *Covert Policing Review* 33.

400 RIPA 2000, s.26(9)(b),(c).

401 Code of Practice, paras 7.103–7.107

402 No 00048539/99, 5 November 2002.

403 But see *McGartland and another v Attorney General* [2014] EWHC 2248 (QB).

404 de Silva, D., *The Report of the Patrick Finucane Review*, December 2012, HC 802-I. Amongst other recent allegations of official collusion in Northern Ireland are: Stevens, J, Stevens Enquiry: *Overview and Recommendations* (Metropolitan Police Service, London, 2003); Police Ombudsman for Northern Ireland, *The Circumstances surrounding the death of Raymond McCord Junior and related Matters* (Belfast, 2007); Lord MacLean, *Billy Wright Inquiry Report* (2010–12 HC 431); Morland, Sir M., *Rosemary Nelson Inquiry* (2010–12 HC 947). See generally Stevens, J, *Not for the Faint-Hearted* (Weidenfield & Nicholson, London, 2005); Rolston, B, 'An effective mask for terror' (2005) 44 *Crime Law & Society* 181; Walker, C., *Terrorism and the Law* (Oxford University Press, Oxford, 2011) chap. 2; Cadwallader, A., *Lethal Allies* (Mercier Press, Dublin, 2013).

1. Scope

137 Although the word **'encryption'** appears in the title of Part III, it is not found anywhere else in sections 49 to 56. The more general term of **'protected information'** is used and defined in section 56(1) as meaning 'electronic data which, without the key to the data (a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily, be put into an intelligible form' The Code of Practice describes it as 'at its simplest the protection of electronic data is undertaken using a password which, if correct, gives access to the data in an intelligible form':[405]

Primarily it is application of cryptography to the confidentiality of data which is exploited by terrorists and criminals to protect their data, whether it is stored data, on a disk or other storage device, or data being communicated from one to another or from one to many others. The measures in Part III are intended to ensure that the ability of public authorities to protect the public and the effectiveness of their other statutory powers are not undermined by the use of technologies to protect electronic information.[406]

138 The references to a key in the present context relates to the **data code** required to enable the data to be accessed. It is defined in section 56(1) as 'any key, code, password, algorithm, or other data the use of which (with or without other keys) allows access to the electronic data or facilitates the putting of it in an intelligible form'. The Code of Practice states 'all manner of material can constitute a key'[407] and dedicates two and a half pages to the subject.[408]

139 Part III of RIPA 2000 empowers public authorities with investigatory remits to require encrypted data to be 'unscrambled' or to hand over the key so that it can be de-coded. Part III also creates offences of failure to comply with any notice served and tipping-off.

140 The **National Technical Assistance Centre (NTAC)**, based in the Security Service, is not referred to in RIPA 2000, but it is designated within the Code of Practice as the 'lead national authority for all matters relating to the processing of protected information into intelligible form and to disclosure of key material'.[409] It must give its prior approval before the public authority can exercise Part III powers which will be accorded only after it assesses the organization as 'competent to exercise [them]'.[410]

2. Issuance

141 A notice requiring disclosure of protected information may be given under section 49 of RIPA 2000 (a 'Section 49 Notice'). The process must be initiated by persons who have appropriate permission within Schedule 2.[411] Paragraph 1 of Schedule 2 creates a mandatory requirement that appropriate permission for the giving of a Section 49 Notice is granted by a judge in writing.[412] It is subject

405 Code of Practice, para.2.3.
406 Code of Practice, para.2.5.
407 Code of Practice, para.3.19.
408 Code of Practice, paras.3.18–3.29.
409 Code of Practice, para.3.10.
410 *Ibid.*
411 The Code of Practice deals with appropriate permission at paras.9.1– 9.33.
412 RIPA 2000, Sch.2, para.1(1).

to various exemptions in the Schedule.[413] In England and Wales, the judge is a Circuit or High Court judge or a District Judge (magistrates' courts); in Scotland, a sheriff; or in Northern Ireland, a county court judge.[414] Any application should specify the grounds on which it is based and describe the information which has been or is likely to be obtained and must explain why it is reasonably believed that the person concerned has possession of a key or keys to the protected information. There is also a requirement to explain why it is not reasonably practicable to acquire or obtain access to the protected information in an intelligible form by other conventional means and to explain to whom the disclosure will be made, how the disclosed material will be handled, stored and safeguarded from unnecessary further disclosure.[415] In an urgent case, the application may be made orally.[416]

142 Where an exemption applies, the **person able to give appropriate permission** should **not be involved in the investigation**, although the Code of Practice recognizes there may be circumstances where this is unavoidable.[417] Any permission granted must be in writing or in a form that produces a record of it.[418]

143 The **first exemption** concerns protected information obtained **under a warrant or an authorization**[419] Where protected information has, or is likely to, come into the possession of a public authority by virtue of the exercise of a statutory power under section 49(1)(a), (b) or (c), which relate to information obtained by means of property interference, interception, or communications acquisition powers, paragraph 2 of Schedule 2 applies 'where the statutory power in question is one exercised, or to be exercised, in accordance with either a warrant issued by the Secretary of State or a person holding judicial office[420] or an authorisation under Part III of the Police Act 1997'.[421] In respect of the former, this is limited to persons holding office under the Crown, the police and Revenue and Customs and entitled to exercise the power conferred by the warrant, or is of the description of persons on whom the power conferred by the warrant was, or could have been, conferred.[422] The latter applies only to the police and Her Majesty's Revenue and Customs.[423] Subject only to two other exceptions,[424] no permission in writing is necessary from a judge in these circumstances provided either the warrant or the authorization contained the relevant authority's permission for the giving of Section 49 Notices in relation to protected information to be obtained under the warrant or authorization, or since the issue of the warrant or authorization, written permission has been

413 RIPA 2000, Sch.2, para.1(2).
414 RIPA 2000, Sch.2, para.1.
415 Code of Practice, para.4.13.
416 Code of Practice, para.4.12.
417 Code of Practice, para.4.10.
418 Code of Practice, paras.4.14–4.16.
419 Code of Practice, paras 9.13–9.17.
420 RIPA 2000, Sch.2, para.2(1)(a); see also the definitions in para.2(6)(a)–(b).
421 RIPA 2000, Sch.2, para.2(1)(b).
422 RIPA 2000, Sch.2, para.2(3), (4).
423 RIPA 2000, Sch.2, para.2(5); see subparas.(6)(c) and (7) as to persons to whom the provisions extend under the Police Act 1997.
424 RIPA 2000, Sch.2, para.6.

granted by the relevant authority for the giving of such Notices in relation to protected information obtained under the warrant or authorization.[425]

144 The **second exemption** relates to protected information obtained by the **intelligence agencies** using their **statutory powers** but **without a warrant**. This relates to the same categories of protected information that are subject to the first exemption, as set out in section 49(1)(a) to (c) but which have come into the possession of any of the intelligence services or are likely to do so; and it is not information in the case of which paragraph 2 applies[426] (the first exemption). No permission in writing from a judge is necessary in these circumstances if written permission for the giving of a Section 49 Notice in relation to that information has been granted by the Secretary of State[427] on the application of a member of one of the intelligence services.[428] This is subject to the general exception in paragraph 6(1)[429] and applies 'where the protected information is in the possession, or is likely to come into the possession, of both any of the intelligence services and a public authority which is not one of the intelligence services'.[430]

145 The **third exemption** relates to protected information obtained **by public authorities** using **statutory powers** but **without a warrant**.[431] This relates to the same categories of protected information that are subject to the first and second exemptions, but also that falling within section 49(1)(d) and is not information also falling within the first three subsections.[432] Section 49(1)(d) relates to protected information that 'has come into the possession of any person as a result of having been provided or disclosed in pursuance of any statutory duty (whether or not one arising as a result of a request for information), or is likely to do so'. No permission in writing from a judge is necessary where the statutory power was exercised, or is likely to be exercised, by the police, the National Crime Agency. or a member of Her Majesty's forces, or the information was provided or disclosed, or is likely to be provided or disclosed, to any of them or the information is in their possession, or is likely to come into their possession.[433]

146 The **fourth exemption** relates to protected information obtained **without** using **statutory powers**. This relates to the category of protected information falling within section 49(1)(e) – information which 'has, by any other lawful means not involving the exercise of statutory powers', come into the possession of any of the intelligence services, the police, National Crime Agency, or Her Majesty's Revenue and Customs, or is likely to come into their possession. No permission in writing from a judge is necessary where the protected information is in or is likely to come into the possession of any of the intelligence services and written permission for the giving of Section 49 Notices in relation to that information has been granted by the Secretary of State.

425 RIPA 2000, Sch.2, para.2(2).
426 RIPA 2000, Sch.2, para.3.
427 RIPA 2000, Sch.2, para.3(2).
428 RIPA 2000, Sch.2, para.3(3)(b).
429 RIPA 2000, Sch.2, para.3(2).
430 RIPA 2000, Sch.2, para.3(3).
431 Code of Practice, paras 9.21–9.22.
432 RIPA 2000, Sch.2, para.4(1).
433 RIPA 2000, Sch.2, para.4(2).

147 The duration of an appropriate permission is limited by the terms upon which it was given.[434] A permission granted by any person under any provision of Schedule 2 does not entitle any person to give a Section 49 Notice at any time after the permission has ceased to have effect.[435] It is the responsibility of the person granting appropriate permission to **specify the duration** of it. Where this is for a lengthy period of time it will need 'careful on-going consideration particularly with regard to whether in the specific circumstances the notice remains necessary and proportionate'.[436]

148 A person with appropriate permission under Schedule 2 who believes, on reasonable grounds, that a key to protected information is in the possession of any person may, serve a Section 49 Notice on that person,[437] provided there is also a belief that the imposition of a disclosure requirement is both necessary in the interests of national security, for the purpose of preventing or detecting crime or in the interests of the economic well-being of the United Kingdom[438] and 'for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty'[439] In addition, he or she must believe on reasonable grounds that the imposition is proportionate to what is sought to be achieved by it,[440] and other than by way of serving a notice that it is not reasonably practicable to obtain possession of the protected information in an intelligible form.[441] A Section 49 Notice may be amended but in restricted circumstances.[442] A notice must be withdrawn by the person with appropriate permission if at any time after giving the notice and before any disclosure is made, it is no longer necessary or proportionate.[443]

149 The effect of a Section 49 Notice is that it imposes on a person who is in possession at a relevant time of both the protected information and a means of obtaining access to the information and of disclosing it in an intelligible form, a disclosure requirement in respect of it.[444] That person is entitled to use any key in his possession to obtain access to the information or to put it into an intelligible form[445] and is required, in accordance with the notice imposing the requirement, to make a disclosure of that information in an intelligible form.[446] Where there is an obligation on a person to make a disclosure of the information in an intelligible form, the obligation is discharged if he or she makes, instead, a disclosure of any key to the protected information that is in their possession and that disclosure is made, to the person to whom, and by the time by which, it was required to be provided in accordance with the Section 49 Notice.[447] If a person is served with a Section 49 Notice but is not in possession of the infor-

434 Code of Practice, paras.9.31–9.33.
435 RIPA 2000, Sch.2, para.7(1).
436 Code of Practice, para.9.32.
437 RIPA 2000, s.49(2)(a).
438 RIPA 2000, s.49(2)(b)(i); applying subs.3.
439 RIPA 2000, s.49(2)(b)(ii).
440 RIPA 2000, s.49(2)(c).
441 RIPA 2000, s.49(2)(d).
442 Code of Practice, para.4.37.
443 Code of Practice, para.4.41.
444 RIPA 2000, s.50(1).
445 RIPA 2000, s.50(1)(a).
446 RIPA 2000, s.50(1)(b).
447 RIPA 2000, s.50(2)(a) and (b).

mation and without a key (which they do not possess), they are incapable of obtaining access to the information and of disclosing it in an intelligible form, or the Section 49 Notice can only be complied with by disclosing the key, the effect of the notice is to require the person to disclose the key.[448] In a case where a Section 49 Notice has been served on a person who has information relating to the whereabouts of the key which they no longer have, they must provide the information that would lead to the discovery of it.[449]

150 The person served must be given a **reasonable and realistic time** within which to comply with the notice but this will vary depending on the facts of the case. This includes time to access legal or technical assistance.[450] In exceptionally urgent cases the time may be curtailed, such as where there is an immediate threat to life or national security or urgent operational requirement.[451]

151 Concern was expressed during the passage of the Regulation of Investigatory Powers Bill that section 49 may breach Article 6 ECHR where compliance with a Notice resulting in disclosure of a key to avoid an offence may **unfairly incriminate the person affected**. The government rejected this argument on the basis that 'the right against self-incrimination does not extend to the use in criminal proceedings of material that may be obtained from the accused [through] the use of compulsory powers, but which has an existence independent of the will of the suspect; for example, documents recovered under a warrant'.[452]

152 In *R v S and A*,[453] the Court of Appeal had no difficulty accepting that the protection against self-incrimination could be engaged by a requirement to comply with a Notice in principle but:

'On analysis, the key which provides access to protected data, like the data itself, exists separately from each appellant's „will". Even if it is true that each created his own key, once created, the key to the data, remains independent of the appellant's „will" even when it is retained only in his memory, at any rate until it is changed. If investigating officers were able to identify the key from a different source (say, for example, from the records of the shop where the equipment was purchased) no one would argue that the key was not distinct from the equipment which was to be accessed, and indeed the individual who owned the equipment and knew the key to it …'[454]

153 However, the Court cautioned that 'If however, as for present purposes we are assuming, they contain incriminating material, the fact of the appellants' *knowledge* of the keys may itself become an incriminating fact.'[455] The Court of Appeal added in dismissing the appeal:

'Although the appellants' knowledge of the means of access to the data may engage the privilege against self-incrimination, it would only do so if the data itself – which undoubtedly exists independently of the will of the appellants

448 RIPA 2000, s.50(3).
449 RIPA 2000, s.50(8) and (9).
450 Code of Practice, paras.4.31–4.33.
451 Code of Practice, para.4.34.
452 Hansard (House of Lords) vol.614 col.972, Lord Bassam.
453 [2008] EWCA Crim 2177.
454 *Ibid.,* para.20.
455 *Ibid.,* para.21.

and to which the privilege against self-incrimination does not apply – contains incriminating material. If that data was neutral or innocent, the knowledge of the means of access to it would similarly be either neutral or innocent. On the other hand, if the material were, as we have assumed, incriminatory, it would be open to the trial judge to exclude evidence of the means by which the prosecution gained access to it. Accordingly the extent to which the privilege against self-incrimination may be engaged is indeed very limited.'[456]

154 There are some cases where the Section 49 Notice will direct that disclosure of the key itself is required.[457] Such a notice can only be imposed if either the person who for the purposes of Schedule 2 granted the appropriate permission for the giving of the notice in relation to that information, or any person whose permission for the giving of a such a notice in relation to that information would constitute the appropriate permission under that Schedule, has given a direction that the Section 49 Notice can only be complied with by the disclosure of the key itself.[458]

155 A direction can **only be given by certain ranks** within the public authority and **on notice to either** the **Intelligence Services Commissioner** or the **Chief Surveillance Officer**.[459] For the police, it is the Chief Constable, in the case of National Crime Authority, it is the Director General, and for Her Majesty's forces it is a brigadier or equivalent rank.[460] The permission can only be granted if they believe there are 'special circumstances of the case which mean that the purposes for which it was believed necessary to impose the requirement in question would be defeated, in whole or in part, if the direction were not given' and the grant is proportionate.[461] Consideration must be given to the extent and nature of any protected information that may also be accessed over and above that which is sought and any adverse effect compliance with the direction may have on any business carried on by the person served with the notice.[462]

156 There are arrangements for an appropriate contribution to be made towards the costs of compliance with a section 49 Notice.[463]

3. Offences

157 It is an offence for a person served with a Section 49 Notice knowingly to fail to make the disclosure required.[464] However, it will not be an offence if the person can show that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it.[465] There is a defence if the accused shows that it was not reasonably practicable for him or her to make the disclosure required before the time by which he or she was required to do so by the Section 49 Notice but he or she did make that disclosure as soon after that time as it was reasonably practicable to do so.[466]

456 *Ibid.,* para.24.
457 RIPA 2000, s.50(3)(c).
458 RIPA 2000, s.51(1).
459 RIPA 2000, s.51(6).
460 RIPA 2000, s.51(2).
461 RIPA 2000, s.51(4).
462 RIPA 2000, s.51(5). See also Code of Practice, para.6.6.
463 RIPA 2000, s.52; see also Code of Practice, paras.4.43 and 4.44.
464 RIPA 2000, s.53(1).
465 RIPA 2000, s.53(2).
466 RIPA 2000, s.53(4).

158 The Chief Surveillance Commissioner reported that in the period 2013–2014[467] thirty-seven approvals were granted by a Circuit judge. Of these thirty three had been served but only seven were complied with. There had been two convictions. These figures are surprisingly low, particularly since the substantive offences include firearms, extremism and child abuse.

159 The offence of **'tipping-off'** is committed under section 54 where a Section 49 Notice contains a requirement to keep secret service of the Notice, its contents and the things done in pursuance of it.[468] The requirement of secrecy may be imposed in two circumstances: first, where it is included with the consent of the person who for the purposes of Schedule 2 granted the appropriate permission for the service of the Notice; secondly, where the person who serves the notice is a person whose permission would have constituted appropriate permission.[469] Section 54(3) limits the circumstances where a requirement of secrecy arises to where the protected information has come or is likely to come into the possession of the police, NCA, Her Majesty's Revenue and Customs or any of the intelligence services 'by means which it is reasonable, in order to maintain the effectiveness of any investigation or operation or of investigatory techniques generally, or in the interests of the safety or well-being of any person, to keep secret from a particular person'.

160 There are **five defences to an offence** under section 54. First, it is a defence for the accused to show that the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure and the accused could not reasonably have been expected to take steps, after being served with the section 49 Notice becoming aware of it or of its contents, to prevent the disclosure.[470] It is also a defence for the accused to show that the disclosure was made by or to a professional legal adviser in connection with the giving of advice about Part III.[471] Thirdly, it is a defence for the accused to show that the disclosure was made by a legal adviser in contemplation of, or in connection with, any legal proceedings.[472] The privilege defences do not apply where privilege does not arise (for instance where a disclosure is made with a view to furthering any criminal purpose).[473] Next, it is a defence for the accused to show that the disclosure was confined to a disclosure made to a relevant Commissioner or authorized by a Commissioner, by the terms of the notice, by or on behalf of the person who gave the notice, or by or on behalf of a person who is in lawful possession of the protected information to which the notice relates and came into possession of that information as mentioned in section 49(1).[474] Finally, it is a defence for an accused (other than the person to whom the notice was given) to show that of knowledge or reasonable grounds for suspecting that the notice contained a requirement to keep secret what was disclosed.[475]

467 *Annual Report of the Chief Surveillance Commissioner, 2013–2014* (2013–14 HC 343) paras.4.13.
468 RIPA 2000, s.54(1).
469 RIPA 2000, s.54(2).
470 RIPA 2000, s.54(5).
471 RIPA 2000, s.54(6).
472 RIPA 2000, s.54(7).
473 RIPA 2000, s.54(8).
474 RIPA 2000, s.54(9).
475 RIPA 2000, s.54(10).

4. Challenges

161 A further challenge to the compatibility of sections 49 and 53 of RIPA and the **protection against self-incrimination** either domestically or in the ECtHR seems inevitable. The decision in *R v S and A* is unlikely to be the last word particularly in light of the influence of international jurisprudence. For instance, in *Re Boucher*,[476] the US District Court for the District of Vermont held that requiring a suspect to provide an encryption code was in breach of his fundamental right against self-incrimination provided by the Fifth Amendment to the US Constitution. It relied heavily on the case of *Doe v US*[477] in which the Supreme Court distinguished between requiring a suspect to provide a physical key to a strongbox containing documents, which may be permissible, and requiring a person to disclose his or her knowledge of the combination to a wall-safe, which was not.

D. Legal liabilities of members of the intelligence services

162 Since litigation is a highly exceptional occurrence for the intelligence agencies, it will be considered in outline only. Forms of external administrative or political oversight are considered more fully in the next section of the paper. Internal oversight is arguably the most important of all, but few details are specified and fewer are divulged. Two important exceptions are, first, the appointment of the **Staff Counsellor to the Intelligence Agencies**, who may receive allegations of abusive conduct from members of the intelligence agencies so as to avert public whistleblowing.[478] Second, the Cabinet Office has issued the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees and Note of Additional Information* in order to guide agents as their relationships with foreign agencies whose methods might involve unacceptable techniques (including torture).[479]

I. Criminal Law

1. Regulation of Investigatory Powers Act 2000

163 Section 1 of RIPA 2000 creates two offences. It is an offence for a person to intercept intentionally any communication at any place in the United Kingdom in the course of its transmission by means of either a public postal or a public telecommunications system unless with lawful authority.[480] The second offence relates to interceptions of communications transmitted by means of a private telecommunications system.[481] The offence is committed if the interception is intentional and takes place without lawful authority[482] but not if the person carrying out the interception is a person with the right to control the operation or

476 (2007) WL 4246473.

477 487 US 201 (1988).

478 Hansard (House of Lords) vol.490, col.811, 30 November 1987.

479 (London, 2010). See also Foreign & Commonwealth Office, *Torture and Mistreatment and Reporting Guidance* (London, 2011) and *Overseas Security and Justice Assistance Guidance* (London, 2014).

480 Section 1(1)(a) and (b).

481 RIPA 2000, s.1(2).

482 RIPA 2000, s.1(2)(a).

the use of the system or has the express or implied consent of such a person to make the interception.[483] The parameters of the right to control the operation or use of the system under section 1(6) were considered by the Court of Appeal in *R v Stanford*.[484] The court held that the trial judge was right to conclude that 'control' was wider than 'the right to operate or use the system' and meant to 'authorise or forbid'. Much of the recent application of section 1 has focused not on the intelligence agencies but on investigative journalists whose activities have been scrutinised by the police in Operations Weeting, Tuleta, Golding and Elveden – involving allegations of hacking into the telephones of celebrities and inappropriate payments to officials by News Group Newspapers and Mirror Group Newspapers.[485]

Next, section 19 creates the offence of **unauthorized disclosures** by persons likely to have access to warrants and/or the content of interceptions from members of the intelligence agencies, police officers, and employees of telecommunications companies. They are required to keep secret the existence and content of warrants and and related matters as well as the actual content of the intercepted material and communications data. **164**

2. Official Secrets Acts 1911–1989

The Official Secrets Acts, enacted in 1911, 1920 and 1989, were mainly designed against **foreign** spies and **internal saboteurs**. However, they can also catch persons such as **intelligence agents** or even **journalists** who **misuse sensitive information by divulging it without official authorisation**. **165**

Section 1 of the 1911 Act applies to any person who engages in 'spying or sabotage' which has been applied not only to foreign spies and double agents[486] but also to demonstrators on defence installations.[487] Sub-sections (1)(b) and (c) have some application to members of the intelligence services. These offences include the creation of, for example, a note, or the communication of it, which is calculated to be, or might be, **useful to an enemy**. The 1920 Act creates various further offences. Section 1 penalises allowing any other person to have possession of any official document or communicate secrets without lawful authority. Aiding and abetting contravenes section 7.[488] **166**

The **misuse of information by officials**, including disclosure of scandals to the press, used to be the subject of further offences under section 2 of the Official Secrets Act 1911, but following a long process of reform,[489] a more modest set of offences has appeared under the Official Secrets Act 1989. Of greatest relevance **167**

483 RIPA 2000, s.1(6)(a) and (b). See further s.4 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, SI 2000/2699.

484 [2006] EWCA Crim 258.

485 See especially *R v Coulson and others* [2013] EWCA Crim 1026. The stream of prosecutions halted in 2015: http://www.cps.gov.uk/news/latest_news/crown_prosecution_service_re_review_of_operation_elveden/index.html; http://www.cps.gov.uk/news/latest_news/no_further_action_to_be_taken_in_operations_weeting_or_golding/.

486 See *R v. Blake* (1961) 45 Cr. App. R. 292; *R v Britten* [1969] 1 WLR 151; *R v Michael Bettany* (*Report of the Security Commission* (Cmnd.9514, London, 1985)).

487 *Chandler v Director of Public Prosecutions* [1964] AC 763; Official Secrets (Prohibited Places) Orders 1955 SI 1955/1497, 1975/182.

488 See *R v Oakes* [1959] 2 QB 350; *R v Bingham* [1983] QB 870.

489 See *Departmental Committee on section 2 of the Official Secrets Act 1911* (Cmnd.5014, London, 1972); *Reform of section 2 of the Official Secrets Act 1911* (Cmnd.7285, London, 1978); *Reform of section 2 of the Official Secrets Act 1911* (Cm.408, London, 1988).

here is section 1(1) (a) which creates an offence for a member of the security and intelligence services, without lawful authority, to disclose any information, document or other article relating to security or intelligence. It is a defence if the person did not know or had no reasonable cause to believe that the matters related to security or intelligence or if the person believed he had lawful authority to disclose and had no reasonable cause to believe otherwise.[490] However, there is **no need to prove that any damage resulted from the disclosure**. It is a further offence under section 8(4) and (5) for a member of the intelligence services to fail to safeguard information. There are further offences applicable to Crown servants and government contractors in section 2, which cover the damaging disclosure of defence related information, in section 3, concerning the damaging disclosure of information relating to international relations and in section 4 concerning criminal activities and special investigative powers.

168 Two notable prosecutions of intelligence agents have arisen under section 1. In ***R v Shayler***,[491] a former security service officer disclosed to a national newspaper some documents relating to intelligence matters, most notably an MI6 plot to assassinate Libyan leader Colonel Gaddafi. Shayler was convicted of offences under sections 1 and 4 of the 1989 Act. The (judicial) House of Lords **dismissed his claim of a defence** that it was, **in the public or national interest to make the disclosure**. Furthermore, given the special position of members of the intelligence services, and the highly confidential nature of information in their possession, the inevitable interference with their right to freedom of expression was required to achieve the legitimate object of acting in the interests of national security allowed by article 10(2). Next, in *R v Keogh*,[492] the defendant, who was employed at GCHQ, acquired information about a meeting between Prime Minister Blair and President Bush concerning policy in Iraq. The defendant photocopied the letter and disclosed it to his co-defendant, a political researcher for a Member of Parliament who disclosed it to the Member of Parliament. The defendant was charged under sections 2 and 3. At a preparatory hearing, the trial judge ruled that the statutory defences, which required a defendant to prove that he did not know and had no reasonable cause to believe that his disclosure related to defence or international relations or that it would be damaging, were compatible with the presumption of innocence guaranteed by article 6 of the European Convention. On appeal, it was accepted that the natural meaning of the defences would be disproportionate and unjustifiable and the sections should be read down under section 3 of the HRA 1998 so as to treat the burden of proof that they imposed on a defendant as no more than evidential.

168a The various offences in the Official Secrets Acts are the subject of consultation by the Law Commission.[493] The main proposals include: **clarification** of the espionage type offences and those related to unauthorised disclosures; increased maximum sentences of some conduct; new measures to protect sensitive sites; the extension of jurisdiction to cover sensitive information which is compromised by conduct abroad; and providing a statutory process for concerns about illegality and impropriety to be independently investigated. It may

490 Official Secrets Act 1989, ss.1(5) and 7(4) respectively

491 [2002] UKHL 11.

492 [2007] EWCA Crim 528.

493 *Protection of Official Data* (Consultation Paper no.230, London, 2017).

be commented that the acute controversies raised by the previous reform attempts, especially the freedom of the press, and the very low rate of prosecutions, render crimes of official secrecy an unpromising field for technical law reform.[494]

3. Other offences

A generic immunity is granted under section 7 of the ISA 1994 to the Intelligence Service or GCHQ in order to excuse under UK civil or criminal law actions for which the agent could otherwise be liable in the United Kingdom for any act done outside the British Islands under a tasking authorisation of the Secretary of State.[495] The actions must be undertaken for the proper discharge of a function of the Intelligence Service and their nature and likely consequences must be reasonable. The intention is **not to grant 'a licence to kill'** (though the position is unclear) but to **allow, for instance, theft, forgery, and bribery** which might otherwise contravene the Criminal Justice Act 1948, section 31: 'Any British subject employed under His Majesty's Government in the United Kingdom in the service of the Crown who commits, in a foreign country, when acting or purporting to act in the course of his employment, any offence which, if committed in England, would be punishable on indictment, shall be guilty of an offence …, and subject to the same punishment, as if the offence had been committed in England.'.[496] **169**

II. Civil Law

The potential **civil liability** of intelligence agencies has begun to impinge on policies and activities much more significantly in recent years. The trend began with the intelligence agencies availing themselves of the civil law to curtail the publication of sensitive information contained in memoirs or leaks of former agents. The cause célèbre is the litigation which surrounded the publication of the memoirs of former Security Service agent, Peter Wright, in his book, ***Spycatcher***.[497] The UK authorities **sought to prevent the publication** of the book based on the equitable doctrine of **breach of confidence**. The litigation was in part successful in the UK but not in other jurisdictions or before the ECtHR.[498] **170**

In *AG v Blake*,[499] **George Blake**, an SIS agent who had spied for the Russians from 1944 until 1961, was convicted under the Official Secrets Act 1911 and **171**

494 See Everett, M., *The Official Secrets Acts and Official Secrecy* (House of Commons Briefing Paper CB07422, London, 2015).

495 But where the property is discovered to be in the UK, the action may continue: Terrorism Act 2006, s.31. A similar amendment relating to apparatus had been made by the Anti-Terrorism Crime and Security Act 2001, s.116.

496 See further Cobain, I., 'How secret renditions shed light on MI6's licence to kill and torture' *The Guardian* 14 February 2012, http://www.theguardian.com/world/2012/feb/14/mi6-licence-to-kill-and-torture.

497 Heinemann, Sydney, 1987.

498 *A.G. v Guardian Newspapers* [1987] 1 WLR 1248, (No.2) [1988] 2 WLR 805, [1988] 3 WLR 776; *Lord Advocate v. Scotsman* [1989] 3 WLR 358; *AG for England and Wales v Brandon Books Publishers* [1987] ILRM 135; *AG for UK v Heinemann Publishers* (1988) 78 ALR 449; *AG for UK v Wellington Newspapers* [1988] 1 NZLR 129; *AG v South China Morning Post* [1989] 2 FSR 653; *Observer, Guardian etc. and Sunday Times (No.2) v UK*, App. nos.13166/87, 13585/88, Ser. A 216, 217 (1991).

499 [2000] UKHL 45. A claim under Art. 6 relating to the length of proceedings (begin in 1991) was upheld in *Blake v UK*, App no.68890/01, 25 October 2005.

sentenced to 42 years' imprisonment. He escaped from prison to Russia in 1966 and later published his autobiography.[500] The Crown successfully claimed that any **profits must be paid to the Crown** on the basis of breach of confidence, breach of contract,[501] and copyright.

172 Next, in 1997, Richard Tomlinson was convicted of an offence contrary to section 1 of the Official Secrets Act 1989. The offence concerned the disclosure of information relating to security or intelligence in the form of the synopsis of a prospective book.[502] The book, *The Big Breach: From Top Secret to Maximum Security*, was published in Moscow in 2001[503] and was subsequently serialised by the *Sunday Times*. On 26 July 2001, the High Court granted an **injunction against publication** of the book in England.[504]

173 Civil law has also been used as a sword against the intelligence agencies as well as a shield in their defence. The techniques of undercover police squads have included the formation of personal and sexual relations with the targets of the operation. The claimants are currently seeking damages for the torts of deceit, assault, misfeasance in public office and negligence, as well as damages for breaches of the HRA 1998.[505] Even more serious, several claims have arisen concerning the collusion by UK intelligence agencies in the torture and other **mistreatment of terrorism suspects** by foreign agencies often in connection with CIA-inspired programmes of **rendition**. The scene was set by the case of Binyam Mohamed.[506] Having been released from Guantanamo Bay in 2009, he brought claims that the UK intelligence agencies had colluded in his interrogation and rendition from Pakistan via Morocco. The claim was resulted in a settlement by the payment of substantial compensation.[507] An inquiry by Lord Justice Gibson found 27 instances of credible allegations.[508] There are also pending cases about collusion in rendition to Libya.[509] However, claims of collusion which would either undermine the safety of a previous criminal conviction[510] or would require judgment on a foreign state[511] have been rejected.

---

500 *No Other Choice* (Jonathan Cape, London, 1990).

501 An injunction on contractual grounds against the memoirs of a special forces soldier, Andy McNab, *Bravo Two Zero* (Bantam Press, London, 1993) was lifted in 1995. See further *R v Attorney General for England and Wales* [2003] UKPC 22.

502 See http://www.cps.gov.uk/news/latest_news/119_07/.

503 Narodny Variant Publishers.

504 *Attorney General v Times Newspapers Ltd* [2001] EWCA Civ 97; *HM Attorney General v Tomlinson* [2002] EWCA Civ 156.

505 *AJA and AKJ v Commissioner of Police for the Metropolis* [2013] EWCA Civ 1342; *DIL and others v Commissioner of Police of the Metropolis* [2014] EWHC 2184 (QB).

506 *R (Binyam Mohammed) v Secretary of State for the Foreign & Commonwealth Office* [2008] EWHC 2048, 2100, 2519, 2549, 2973 (Admin), [2009] EWHC 152 (Admin). See Joint Committee on Human Rights, *Allegations of UK complicity in torture* (2008–09 HL 152/HC 230) and *Government Reply* (Cm.7714, London, 2009); Cobain, I., *Cruel Britannia: A secret history of torture* (Portobello Books, London, 2012).

507 Hansard (House of Commons) vol.518 col.752 16 November 2010, Kenneth Clarke.

508 Gibson, P., *The Report of the Detainee Inquiry* (Cabinet Office, London, 2013). They await examination by the ISC: http://isc.independent.gov.uk/news-archive/11september2014.

509 *Belhaj & Boudchar v Straw* [2013] EWHC 2672 (QB), [2014] EWCA Civ 1394; *Belhaj v Security Service* (IPT/13/132–9H, 7 February 2014).

510 *Amin v DG of Security Service* [2015] EWCA Civ 653.

511 *R (Khan) v Secretary of State for Foreign and Commonwealth Affairs* [2014] EWCA Civ 24.

This outbreak of offensive civil litigation has caused considerable discomfort to the intelligence agencies not only because of the disquieting allegations but also because the process of disputation requires the disclosure of sensitive information about techniques, personal identities, and linkages to foreign agencies. Some of these challenges could be met by the invocation of the common law doctrine of public interest immunity by which material evidence can be withheld from a claimant in the interests of national security but only at the cost of not being able to use the evidence in defending against the claim.[512] Some solace has been granted to the embattled intelligence agencies by way of the introduction into civil proceedings of Closed Material Procedures by the Justice and Security Act 2013.[513] **174**

E. Oversight

I. Commissioners

The notion of a judicial commissioner to oversee the activities of the intelligence agencies in the United Kingdom was conceived following the decision in *Malone v Commissioner of the Metropolis (No. 2)*[514], a case concerning allegations of phone tapping by the police. The judgment prompted the appointment of a judicial monitor of interceptions,[515] Lord Diplock, whose first report in 1981[516] reaffirmed that, in his opinion, the current system protected individual privacy rights. Over thirty years on, no subsequent Commissioner has reached a different view. Legislation, somewhat inevitably, confirmed these arrangements. The Interception of Communications Act 1985, section 8, created the post of **Interception of Communications Commissioner**. These provisions were the subject of a successful challenge in *Liberty and Others v United Kingdom*.[517] Other commissioners were created by the Security Service Act 1989, the ISA 1994, and the Police Act 1997. Save for the latter, they have now been replaced with new posts under the RIPA 2000, creating a network which is not entirely unified and certainly not simplified.[518] At present, RIPA 2000, Part IV, makes provision for the 'Scrutiny etc. of Investigatory Powers and of the Functions of the Intelligence Services'. **175**

1. Interception of Communications Commissioner

The Interception of Communications Commissioner is a Prime Ministerial appointment.[519] The appointee must hold high judicial office.[520] In addition to being required to provide the assistance to the IPT,[521] the Commissioner has **176**

512 See McKay, S., *Covert Policing: Law and Practice*, (2nd ed., Oxford University Press, Oxford, 2014) chap. 9.

513 See Tomkins, A., 'Justice and Security in the United Kingdom' (2014) 47 *Israel Law Review* 305; Walker, C., 'Living with National Security Disputes in Court Processes in England and Wales' in Martin, G., Scott Bray, R., and Kumar, M., *Secrecy, Law and Society* (Routledge, Abingdon, 2015).

514 [1979] Ch 344.

515 See *The Interception of Communications in Great Britain* (Cmnd.7873, London, 1980).

516 Cmnd.8191, London, 1981.

517 App. no.58243/00, 1 July 2008.

518 See Information Commissioner, *Surveillance Road Map*, https://www.gov.uk/government/publications/surveillance-road-map.

519 RIPA 2000, s.57(1).

520 RIPA 2000, s.57(5)

521 RIPA 2000, s.57(3).

four additional functions. The first three involve keeping under review the exercise and performance by the Secretary of State, first, in relation to the exercise of powers under sections 1 to 11 and secondly, in relation to information obtained under Part 1 or Part III of RIPA.[522] The Commissioner must also keep under review the exercise and performance of those persons carrying out work under Chapter II of Part 1.[523] Finally, the Commissioner is mandated to keep under review the duty on the Secretary of State to ensure that there are appropriate restrictions on the use of intercept material under section 15 and encryption keys under section 55.[524] The Commissioner also provides oversight of the interception of communications in prisons in England, Wales and Northern Ireland[525] and, since March 2015, directions under the Telecommunications Act 1984, section 94.[526]

177 Individuals engaged in the implementation of interception warrants, ranging from the issuance of a warrant to the practical steps involved in intercepting communications,[527] are all required under section 58(1) to cooperate with the Commissioner.

178 Where it appears to the Commissioner that there has been a breach of RIPA which has not been the subject of a report made to the Prime Minister by the IPT, the Commissioner is required to report to the Prime Minister.[528] The same applies to the requirements under sections 15 and 55.[529] In any event, the Commissioner is required to prepare an annual **report to the Prime Minister**,[530] but may also issue reports about any other matter touching on his functions.[531] The report of the Commissioner is laid **before Parliament**.[532] The Prime Minister and the Commissioner consult on those aspects of the report which should not be published because of the sensitivity of the information.[533] In those circumstances, the Prime Minister can exclude those matters from the copy of the report laid before Parliament.

2. Intelligence Services Commissioner

179 Similar provisions exist in relation to the post of Intelligence Services Commissioner, another Prime Ministerial appointment.[534] It is the function of this officer, who must hold high judicial office,[535] to keep under review **those matters not kept under review by the Interception Communications Commissioner**[536] that relate to the exercise by the Secretary of State of his powers under

522 RIPA 2000, s.57(2)(c).
523 RIPA 2000, s.57(2).
524 RIPA 2000, s.57(2)(d)(ii).
525 It has been recommended that this activity be made statutory: Interception of Communications Commissioner, *2013 Annual Report*, (2013–14 HC 1184) para.7.2.
526 Interception of Communications Commissioner, *2014 Annual Report* (2014–15 HC 1113) para.2.1.
527 The persons are identified in RIPA 2000, s.58(1)(a)–(j).
528 RIPA 2000, s.58(2)(b).
529 RIPA 2000, s.58(3).
530 RIPA 2000, s.58(4).
531 RIPA 2000, s.58(5) and (5A).
532 RIPA 2000, s.58(6) and (6A).
533 RIPA 2000, s.58(7).
534 RIPA 2000, s.59(1).
535 RIPA 2000, s.59(5).
536 RIPA 2000, s.59(2).

sections 5–7 of the ISA 1994.[537] In addition the Commissioner reviews the exercise and performance of the Secretary of State in connection with the activities of the intelligence services and the activities of officials of the Ministry of Defence and of members of Her Majesty's forces, **other than in relation to their deployment in Northern Ireland**, in relation to the Parts II and III of RIPA 2000.[538] The Intelligence Services Commissioner also reviews the activities of members of the intelligence services, officials of the Ministry of Defence and members of Her Majesty's forces in connection with the powers and duties imposed on them under Parts II and III of RIPA.[539] As with the Interception of Communications Commissioner, the Intelligence Services Commissioner must review the adequacy of the arrangements under section 55.[540]

180 As amended by section 5 of the Justice and Security Act 2013, section 59A of RIPA 2000 requires expanded oversight parameters. Section 59A provides that the Commissioner must review the carrying out of any aspect of the functions of the intelligence services,[541] a head of an intelligence service,[542] or any part of Her Majesty's forces, or the Ministry of Defence, so far as engaging in intelligence activity.[543] Section 59A additionally allows for the Commissioner's functions to be added to by direction from the Prime Minister.[544] A direction was issued in 2014 to review the *Consolidated Guidance* relating to overseas cooperation.[545]

181 In all other respects, the functions and duties of the Intelligence Services Commissioner are in the same terms as those of the Interception of Communications Commissioner.[546] However, there is no provision that corresponds with section 58(2) or in subsection (3) (the duty to report to the Prime Minister contraventions or in adequacy in the arrangements).

182 There are **practical limits** in the application of oversight. The Commissioner does not examine the reasoning behind such issuances, nor does he see a substantial proportion of the issued warrants: 'The total number of warrants and authorisations approved across the intelligence services and the MOD in 2013 was 1887. Provided with details of all warrants, I scrutinised 318 warrants extant and paperwork during 2013, 16.8% of the total.'[547]

3. Investigatory Powers Commissioner for Northern Ireland

183 Section 61 of RIPA 2000 establishes an Investigatory Powers Commissioner for Northern Ireland. This appointment is made after consultation with the Prime Minister and the First Minister and Deputy First Minister in Northern Ireland[548] and his function is to keep up the review of the exercise of performance in Northern Ireland by persons on whom they are conferred or imposed of any of

537 RIPA 2000, s.59(2)(a).
538 RIPA 2000, s.59(2)(b).
539 RIPA 2000, s.59(2)(c)–(d).
540 RIPA 2000, s.59(2)(e).
541 RIPA 2000, s.59A(1)(a).
542 RIPA 2000, s.59A(1)(b).
543 RIPA 2000, s.59A(1)(c).
544 RIPA 2000, s.59A(4).
545 Hansard (House of Commons) vol.588 col. 48ws 27 November 2014, David Cameron.
546 RIPA 2000, s.59(3)–(8) mirror the corresponding subsections in s.57.
547 Sir Mark Waller, *Report of the Intelligence Services Commissioner for 2013* (2013–14 HC 304), p. 35.
548 RIPA 2000, s.61(1).

the powers or duties under Part II of RIPA.[549] No appointment has ever been made.[550]

184 Following the **transfer** of responsibility for national security in Northern Ireland under the terms of the St Andrews Agreement 2006 **from the police to the MI5** in 2007, Lord Carlile was appointed (and reappointed in 2013) to review annually the operation of the arrangements for national security matters. Publication tends to be very truncated.[551]

4. Surveillance Commissioners

185 The office of Chief Surveillance Commissioner (or Chief Commissioner) is created by the Police Act 1997, section 91. The appointment is by the Prime Minister, and the appointee must hold high judicial office. The Prime Minister may also appoint such number of other commissioners as he thinks fit (called ordinary commissioners). Additionally, after consultation with the Chief Surveillance Commissioner, the Prime Minister may further appoint under RIPA 2000, section 63, assistant surveillance commissioners.[552] The Surveillance Commissioners together form the Office of Surveillance Commissioners.[553] The core function of a Commissioner is to consider **whether to give approval to an authorisation for a warrant to enter property which is used wholly or mainly as a dwelling or as a bedroom in a hotel**.[554] Since the powers under the Police Act 1997 are exercised by the police and not the intelligence agencies, no further details will be given here other than to note the doubts expressed about the efficacy of the system.[555]

II. Investigatory Powers Tribunal ('IPT')

186 The Investigatory Powers Tribunal ('IPT') is established under section 65. Membership of the IPT and the terms of appointment are set out in Schedule 3 of RIPA 2000. Its jurisdiction is delineated in section 65(2) and relates to complaints 'by a person who is aggrieved by any conduct' **concerning property, communications**, or the **use of any postal service, telecommunications service** or telecommunication system which has been carried out by or on behalf of any of the intelligence services. The IPT is also the only appropriate tribunal for the purposes of section 7 of HRA 1998 in relation **to claims about actions incompatible with Convention rights**. In *R (on the application of A) v B*,[556] the facts related to a manuscript written by a former member of the Security Service who had then been refused permission to publish by the Director of Establishments (human resources head). The claimant brought proceedings for judicial review, but the government responded that the appropriate forum for the dispute was the IPT. The UK Supreme Court held that section 65(2) conferred

549 RIPA 2000, s.61(2).

550 Connolly, P., 'Northern Ireland needs a „snooping" commissioner to monitor RIPA' *Belfast Telegraph* 24 October 2014.

551 See for example Hansard (House of Commons) col.436ws 20 March 2015.

552 See Police Act 1997, s.107.

553 See https://osc.independent.gov.uk/.

554 Police Act 1997, s.97.

555 See Vikram Dodd 'Government's defence of surveillance unconvincing, says ex-watchdog' *The Guardian* June 18 2014 http://www.theguardian.com/world/2014/jun/18/government-surveillance-watchdog-loopholes.

556 *R (on the application of A) v B* [2009] UKSC 12.

exclusive jurisdiction on the IPT to hear proceedings against any of the intelligence services for the purposes of proceedings pursuant to section 7 of the HRA 1998. The Court viewed it as unlikely that Parliament had intended to leave it to the complainant to choose whether to bring proceedings in court or before the IPT. Furthermore, the need to safeguard the secrecy and security of sensitive intelligence material pointed to toward the IPT which had mechanisms to protect sensitive information not available in the mainstream courts.[557]

'Conduct' is further defined in section 65(5) and includes that by or on behalf of the intelligence services,[558] conduct under Parts 1 and II,[559] the giving of encryption notices,[560] and property interferences.[561] It now also extends to the carrying out of surveillance by a foreign police or customs officer.[562] This is defined in section 76A and in summary relates to lawful surveillance carried on outside the United Kingdom but which needs, temporarily, to be carried out here and it is not practicable to obtain authorization under RIPA 2000. Challengeable circumstances are defined in section 65(7) and (7A). The former relates to conduct that was or ought to have been authorized under RIPA and the latter conduct under section 76A. The IPT also has jurisdiction to consider and determine any complaints that come within sub-section 65(4) (the interception of communications),[563] to consider and determine any reference to them by any person who has suffered detriment as a consequence of the operation of the prohibition in section 17 of RIPA 2000 and to hear and determine any such proceedings falling within sub-section 3 as may be allocated to them in accordance with provision made by the Secretary of State by order.[564] (Sub-section 3 is the provision already referred to in relation to proceedings against the intelligence services or arising out of loss or damage relating to encryption.) **187**

The IPT regards its own jurisdiction as falling into **four distinct areas**.[565] First, it investigates complaints against the use of all powers under RIPA 2000. Second, it will investigate any infringement of human rights that may have occurred through using RIPA 2000 powers. Thirdly, the IPT can investigate anything that may have taken place where a provision of RIPA has been relied upon. Finally, the IPT can investigate complaints against any alleged conduct by or on behalf of the intelligence services. **188**

The IPT can **decline to hear a complaint** or reference if it is **frivolous** or **vexatious**.[566] Equally, the IPT has the discretion not to consider any complaint made if it is made more than one year after the conduct to which it relates. When the IPT hears any proceedings under section 65, the principles that a court would apply on application for judicial review should operate.[567] Distinctive features of its procedures include: that it can receive and consider evidence in any form, even if inadmissible in an ordinary court; that it adopts an inquisi- **189**

557 See Investigatory Powers Tribunal Rules 2000, SI 2000/2665.
558 RIPA 2000, s.65(5)(a).
559 RIPA 2000, s.65(5)(b)–(d).
560 RIPA 2000, s.65(5)(e).
561 RIPA 2000, s.65(5)(f).
562 RIPA 2000, s.65(5)(ca).
563 RIPA 2000, s.65(2)(b).
564 RIPA 2000, s.65(2)(d).
565 http://www.ipt-uk.com/section.aspx?pageid=3.
566 RIPA 2000, s.67(4).
567 RIPA 2000, s.67(2).

torial process to investigate complaints, unlike the adversarial approach followed in ordinary court proceedings; and that since it is required to keep from disclosure sensitive materials, closed procedures are allowed.[568] Where the IPT finds for a complainant, it is required to provide them with a summary of the determination and findings of fact.[569] If the activity complained about involves approval by a Secretary of State, the IPT is required to make a report of its findings to the Prime Minister. The IPT may hold 'no determination in favour';[570] as the IPT website explains:

'This prevents criminals, terrorists or foreign intelligence operatives making serial applications to the IPT in order to find out whether they are under investigation and, if they are, how they can avoid detection. Unless the IPT has found that there was a breach of the law by the public authority in question, RIPA does not allow the IPT to disclose whether someone is of interest to the intelligence or law enforcement agencies or to disclose what evidence it has taken into account in considering the complaint or claim.'[571]

190 Where a complaint is investigated, the IPT can issue **legally binding notices** to the relevant public authority requiring it to search for and provide information.[572] The IPT has power to make any interim orders under subsection 67(6). The IPT has powers under subsection 7 on making any adverse finding against the state to award compensation or make other orders as they think fit but has no power to award costs.[573] The IPT can also require the various commissioners with oversight responsibility for the work of the intelligence agencies and others to provide it with all such assistance as it requires.[574]

191 Otherwise than by way of ministerial order, there is **no appeal or judicial review** of the IPT's decision-making, however the Secretary of State is under a duty to provide for an order under section 67(9) that at all times there is recourse for an individual to appeal to a court against the exercise by the IPT of their jurisdiction under section 65(2)(c) (the operation of section 17) and, under section 65(2)(d), any such other proceedings as the Secretary of State may by order subsequently enact.

192 The most significant challenges to the IPT's jurisdiction and procedure are cases IPT/01/62 and IPT/01/77 of 23 January 2003. The cases considered the applicability of Convention rights and common law principles, the legality of the rules and their construction, the ambit of the IPT's discretion and the exercise of any such discretion. These rulings were considered in *Liberty and others v United Kingdom*.[575]

193 As for the applicability of the rules of due process under the Convention and common law principles to the IPT's procedures, the IPT considered not just fair trial rights under article 6 but also whether procedural requirement flowed from the nature of the qualified rights also engaged, namely Articles 8 and 10. The

568 See RIPA 2000, ss.68, 69; Investigatory Powers Tribunal Rules 2000, SI 2000/2665. The Rules do not mention special advocates.

569 RIPA 2000, s.68(4)(a).

570 RIPA 2000, s.68(4)(b).

571 http://www.ipt-uk.com/section.aspx?pageid=4.

572 RIPA 2000, s.68(6).

573 *W v Public Authority* IPT/09/134/C, 1 February 2011.

574 RIPA 2000, s.68(2).

575 App. no.58243/00, 1 July 2008.

crux of the case on the first issue was Rule 9(6), which requires the IPT's proceedings, including oral hearings, to be conducted in private. In the IPT's judgment, the critical question was whether, in making the rules, the Secretary of State had the proper regard he was required to have to the considerations in section 69(6)(a) and (b). These provisions imposed the mandate on the Minister to ensure the proceedings were properly heard and considered but also that no disclosure is made that could damage the public interest or national security. The IPT concluded that the Secretary of State had gone too far in limiting Rule 9(6) in the way he did. The fact that Rule 9(6) was a blanket rule was of itself fatal to its validity. It was *ultra vires* section 69 of RIPA 2000 and consequently did not bind the IPT.[576] They were entitled to exercise their discretion under section 68(1) to hear legal arguments in public under Rule 9(3) subject only to the requirements under Rule 6(1) (the duty not to disclose information contrary to the public interest).

194 In respect of other departures from the normal adversarial procedure (such as for example, exchange of witness statements or evidence), the IPT was satisfied that the rules were within the powers conferred under section 69(1) of RIPA 2000.

195 The IPT has discretions under section 68(1) in respect of three areas of procedure: whether to hold an oral hearing with all parties present; whether to hold the hearing in public; and whether to publish detailed reasons for their rulings on pure questions of law concerning procedure and practice. This is determined by the provisions of section 69(6), the duties of the IPT under the Act and the rules and the particular importance of maintaining the **Neither Confirm Nor Deny policy**.[577] The procedure for the IPT to hold an oral hearing of the preliminary hearing in the presence of all parties, by directing that the oral hearing of the legal argument on the preliminary issues should be treated as having been held in public and by then directing that the reasons for the rulings on preliminary issues should be given in public.[578]

III. Challenges

196 Both the IPT and the collection of Commissioners have been criticised. The array of Commissioners is complex and manages **only partial oversight** in two senses. One is that the impact of the Commissioners is *post hoc*, and there is no prior judicial authorisation of most covert and intrusive activities under RIPA 2000. However, prior judicial review has not been required by the European Convention.[579] The Commissioners' review is partial in a second sense, namely, that not all cases are reviewed. The Commissioners scrutinise all intrusive surveillance authorisations and warrants for property interference, but not, because of the volume of cases and lack of resources,[580] all directed authorisations or the use of CHIS, though if prosecutions result, then the courts will conduct a further check.[581]

576 IPT/01/62 and IPT/01/77, para.173.

577 IPT/01/77, para.195.

578 IPT/01/77, para.205.

579 *Christie v United Kingdom*, App no. 21482/93, 78 -A DR 119 (1994); *Esbester v United Kingdom*, App. no.18601/91, (1993) 18 EHRR CD 72.

580 See Chief Surveillance Commissioner, *2012–13 Annual Report* (2012–13 HC 577) para.3.2.

581 See *R v Harmes and Crane* [2006] EWCA Crim 928; *R v Bard* [2014] EWCA Crim 463.

197 As for the IPT, its secretive processes make it hard to inspire confidence, as does the **very low success rate**,[582] though the view of the IPT itself is that it has 'sought to balance demands for open justice with the necessary protection of sensitive material'.[583] In any event, complaints to the IPT are dampened by the fact that there is never any disclosure to the target of the surveillance activity, though disclosure is not required by the European Convention.[584] Other problems include the **lack of any appeal structure**, leaving the technicalities of judicial review or the remoteness of Strasbourg hearings as the only backstops.

IV. Intelligence and Security Committee ('ISC')

198 The ISC is 'the principal mechanism for providing parliamentary oversight of the agencies.'[585] It was established by the Intelligence Services Act 1994, section 10. The scheme has been amended by Part I of the Justice and Security Act 2013. The ISC comprises nine members who are drawn from both the House of Commons and House of Lords on the nomination of the Prime Minister (who is required to consult with the Leader of the Opposition) with a chair chosen by its members; Ministers of the Crown are excluded.[586]

199 Its purpose is to **examine the policy, administration and expenditure of the intelligence agencies**[587] and otherwise oversee other activities of the government in relation to intelligence or security matters. The ISC also examines the intelligence-related work of the Cabinet Office including the Joint Intelligence Committee and the National Security Secretariat. It also provides oversight of Defence Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism in the Home Office. The remit can also cover any **operational matter** but only so far as: the ISC and the Prime Minister are satisfied that the matter is **not part of any ongoing intelligence** or **security operation**, and is of **significant national interest**; the **Prime Minister has asked the ISC** to consider the matter; or the ISC's consideration of the matter is limited to the consideration of **information provided voluntarily** to the ISC by the intelligence agencies or a government department.[588] Its powers to call for information are set out in Schedule 1, as well powers to take evidence under oath, and it can also commission its own experts, though independent expertise has been difficult to locate. Aside from particular operational matters, the intelligence agencies should supply information as requested by the ISC unless the Secretary of State has decided that it should not be disclosed.[589] The Secretary of State may withhold sensitive information[590] and information which, in the interests of

582 11 cases out of 1469 from 2001–12: McKay, S., *Covert Policing: Law and Practice*, (2nd ed, Oxford University Press, Oxford, 2014) p. 386. The IPT dealt with 756 complaints from 2010–2013 inclusive; it upheld 6 complaints, 283 were ruled no determination, and 336 were ruled frivolous or vexatious: Data abstracted from IPT Annual Case Statistics http://www.ipt-uk.com/section.aspx?pageid=5.

583 *Report 2010* (http://www.ipt-uk.com/docs/IPTAnnualReportFINAL.PDF) p. 18.

584 See *Malone v UK*, App no. 8691/79, Ser A 82 (1984)

585 Bochel, H. et al., 'New mechanisms of independent accountability: Select Committees and Parliamentary scrutiny of the intelligence services' (2015) 68 *Parliamentary Affairs* 314, 314.

586 Justice and Security Act 2013 s.1.

587 *Ibid*., s.2.

588 *Ibid*., s.2(3).

589 *Ibid.,* Sched.1 para.4.

590 As defined, Sched.1 para.5.

national security, should not be disclosed as well as information covered by the normal rules applying to disclosure a Departmental Select Committee of the House of Commons.

The ISC makes an **annual report** to Parliament and may make such other reports to Parliament as it considers appropriate.[591] Before making a report to Parliament, the ISC must send it to the Prime Minister. The ISC must exclude any matter from any report to Parliament if the Prime Minister, after consultation with the ISC, considers that the matter would be prejudicial to the continued discharge of the functions of the intelligence agencies.[592] **200**

The 2013 reforms to the ISC were designed to bring it more into line with **parliamentary select committees**. They began with the Green Paper, *Governance of Britain*,[593] and some (fairly minor) changes were implemented prior to the 2010 General Election.[594] Then, in October 2011, the Ministry of Justice published the *Justice and Security Green Paper*.[595] The Green Paper acknowledged that criticism of the ISC had persisted.[596] The fact that it answered to the Prime Minister fuelled the impression that it was insufficiently independent. Prior to the 2015 General Election, it was notable that 23 of the 39 parliamentarians who have served on the ISC have held ministerial office before being appointed to the committee, 'with a clear preference for members with ministerial experience in defence, foreign affairs and Northern Ireland.'[597] Other criticisms included insufficient knowledge of the operational work of the agencies and a lack of expert support staff.[598] **201**

After the **Justice and Security Act 2013** reforms, the **ISC is a committee of Parliament** (albeit not a normal parliamentary select committee) with increased powers and remit.[599] However, the reservations about its clout were then exacerbated by revelations and allegations around the interception and surveillance programmes operated by the agencies (following the disclosures by Edward Snowden). Shortly after the Snowden revelations, the ISC issued a somewhat precipitate statement in July 2013.[600] It indicated that it had taken 'detailed evidence from GCHQ' and that it had scrutinised 'GCHQ's access to the content of communications, the legal framework which governs that access, and the arrangements GCHQ has with its overseas counterparts for sharing such infor- **202**

591 *Ibid.,* s.3.

592 *Ibid.,* s.3(5). See also Sched.1 para.6.

593 (Cm.7342, London, 2008).

594 See Defty, A., 'Educating Parliamentarians about Intelligence: The Role of the British Intelligence and Security Committee' (2008) 64 *Parliamentary Affairs* 621.

595 (Cm.8194, London, 2011). See: Leigh, I., 'Rebalancing Rights and National Security: Reforming UK Intelligence Oversight a Decade after 9/11' (2012) 27 *Intelligence and National Security* 722.

596 See Joint Committee on Human Rights, *Allegations of UK Complicity in Torture* (2008–09 HL 152/HC 230), *Counter-Terrorism Policy and Human Rights: Bringing Human Rights Back* (2009–10, HL 86 / HC 111).

597 Defty, A., 'It is time to adopt a different approach to appointing members of the Intelligence and Security Committee' *Democratic Audit* 24 March 2015.

598 See Horne, A., 'Security services under the microscope' (2010) 174 *Criminal Law and Justice Weekly* 757.

599 See Bochel, H., et al., 'New mechanisms of independent accountability' (2015) 68 *Parliamentary Affairs* 314.

600 See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf. These matters remain the subject of legal challenges before the ECtHR: *Liberty v UK*.

mation.' Amongst other things it considered allegations 'that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications.' The ISC stated that 'from the evidence we have seen, we have concluded that this is unfounded.'

203 The 2013 reforms have not significantly altered the perception of the **inadequacies of the ISC**. Those critics include the House of Commons Home Affairs Committee, which expressed 'concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability, and to the credibility of Parliament itself'.[601] Credibility was not assisted by the resignation of the ISC Chair, Sir Malcolm Rifkind, in February 2015 after the media had revealed that he had offered to utilise his position as a senior politician on behalf of a fictitious Chinese company (an obvious potential security risk) in return for substantial financial payments.[602]

204 As for work undertaken since the 2013 reforms, two major reports have appeared. The first was the *Report on the intelligence relating to the murder of Fusilier Lee Rigby*,[603] in which detailed attention was given to the relations between the activities of the killers and the actions of the intelligence agencies. The ISC was critical of monitoring procedures by Communications Service Providers (such as Facebook), though serial investigations by the Security Service were excused as sufficiently thorough, especially because, as pointed out even by GCHQ,[604] true intent can be very difficult to discern from online communications. In summary, the ISC's work here was commendable for documenting in detail the failures of security; however, the conclusions drawn might be viewed as at best misplaced and at worst deflecting attention from the shortcomings of the UK's intelligence agencies and blaming instead a foreign scapegoat.

205 The second report, *Privacy and Security: A modern and transparent legal framework*,[605] also bore some promising signs of greater transparency, as evidenced by the substantial list of external witnesses invited to make submissions to the inquiry arising from the Snowden revelations. In substance, this Report reveals a small number of security staff had been disciplined for misusing their surveillance powers, and it further reassures that mass surveillance is not being conducted. However, the ISC does find that the existing legal powers could be construed as providing the agencies with a 'blank cheque to carry out whatever activities they deem necessary',[606] a belated discovery for a review body which was established under the same legislation.

V. Security Commission

206 The Security Commission[607] is a non-statutory device which can be invoked entirely at the behest of the Prime Minister and can be directed to inquire and report on security issues relating, *inter alia*, to the intelligence agencies. Its

601 *Counter-terrorism*, (2013–14, HC 231) para.157.

602 The House of Commons Standards Committee subsequently found no breaches of Parliamentary rules (*Sir Malcolm Rifkind and Jack Straw* (HC 2015–16, 472), but Ofcom concluded that the media had represented the issue fairly (*Ofcom Broadcast Bulletin* (Issue number 295, London, 2015) p. 47).

603 *Report on the intelligence relating to the murder of Fusilier Lee Rigby* (2014–15 HC 795).

604 *Ibid*., para.393.

605 (2014–14 HC 1075).

606 *Ibid*., p 117.

607 Leigh, I., and Lustgarten, L., 'The Security Commission' [1991] *Public Law* 215.

main diet has been to investigate the administrative implications of breaches of security by individuals.[608] The **ISC** seems to have **gained primacy over policy review**, and relatively few Security Commission reports have appeared in recent years.[609]

F. Pending reforms

I. Reports

Three reports issued in 2015 have called for wholesale change. First, the Intelligence and Security Committee, in *Privacy and Security: A modern and transparent legal framework*,[610] called for widescale but rather amorphous changes, as discussed above. The second report, which had been commissioned by the former Deputy Prime Minister, Nick Clegg, was published in July 2015 by the Royal United Services Institute (RUSI) and was entitled *A Democratic Licence to Operate*. This report had the misfortune that its chief backer had been removed from government, and it was in any event far less detailed, cogent, and authoritative than the third report which had already set the scene when published a month earlier. **207**

The third report, *A Question of Trust – Report of the Investigatory Powers Review*, was commissioned by the Home Office and authored by the **Independent Reviewer of Terrorism Legislation**, David Anderson[611] He found that RIPA is 'incomprehensible to all but a tiny band of initiates', concluding that 'This state of affairs is undemocratic, unnecessary and – in the long run – intolerable.'[612] At the same time, recognising both the power of investigatory powers for effective law enforcement and national security and also the need for controls and trust, a **long list of recommendations** is set out. Amongst the most important are that a new law comprehensive legal code is required. Enhanced powers (such as proposed in the draft Communications Data Bill 2012) need to be proven by a detailed operational case. In the meantime, the bulk collection capabilities of GCHQ should continue, but subject to additional safeguards and to the addition of a new explicit power to collect only communications data in bulk. The extraterritorial effect in DRIPA 2014 section 4 should remain, but measures to improve the cooperation of overseas (especially US) service providers and the **development of a new international framework for data-sharing among like-minded democratic nations** must be pursued. As for intercepts, they should be subjected to judicial authorisation (by Judicial Commissioners). Judicial authorisation should also apply to novel and contentious requests for communications data, and to requests for privileged and confidential communications. Next, the three existing Commissioners' offices should be replaced by an **Independent Surveillance and Intelligence Commission**. This body would **208**

608 See *G.A. Prime* (Cmnd.8876, London, 1983) (GCHQ); *Sir Roger Hollis* (Cmnd.8450, London, 1982); *M.J. Bettaney* (Cmnd.9514, London, 1985) (Security Service); *9th Signals Unit and Other Static Communications Units* (Cmnd.9923, London, 1986) (defence; see also Calcutt, D., *Inquiry into the Investigations Carried Out by the Service Police in Cyprus in February and March 1984* (Cmnd.9781, London, 1986).

609 See *Ryan Parry* (Cm.6177, London, 2004).

610 (2014–14 HC 1075).

611 (Home Office, London, 2015). See also Anderson, D., 'The Investigatory Powers Review' [2015] *European Human Rights Law Review* 331.

612 *Ibid.*, para.35.

comprise a new, powerful, public-facing and inter-disciplinary intelligence and surveillance auditor and regulator whose judicial commissioners would take over responsibility for issuing warrants, for authorising novel, contentious and sensitive requests for communications data and for issuing guidance. There would also be an expanded jurisdiction for the Investigatory Powers Tribunal, and a right to apply for permission to appeal its rulings.

II. Investigatory Powers Bill 2015–16 and Investigatory Powers Act 2016

209 The Queen's Speech to Parliament in May 2015 promised a new Investigatory Powers Bill to 'modernise the law on communications data' and it duly appeared as a **draft in November 2015**.[613] Given the size of the undertaking (with over 200 clauses and several schedules), and given that, by the deadline for this paper, the drafts had yet to be subjected to Parliamentary scrutiny, no more than an outline will be attempted here. Despite the wide compass, the exercise is still not comprehensive. The focus is on the interception powers of RIPA 2000 and so only Part I, the Data Retention and Investigatory Powers Act 2014 is replaced wholesale. Conversely, the Bill is almost entirely **silent** on subjects such as **CHIS** and **encryption**. Nevertheless, the wider compass does allow for the clearer statutory regulation of some forms of covert activities which were avowed by the Government only as recently as early 2015. These powers relate to such as bulk data collection from the telecoms companies (currently exercised under section 94 of the Telecommunications Act 1984) and the bulk acquisition of big data sets (such as telephone subscribers and so on) under the general tasking powers of the Security Service Act 1989 and the Intelligence Services Act 1994. Aside from codification, the second principal objective of the Bill is to increase safeguards and oversight. Undoubtedly, it goes further than RIPA 2000, but not so far as critics (including Anderson) had wished.

210 Interception powers are divided between those which are targeted (now under section 8(1) of RIPA 2000) and those which deal in bulk with thematic targets (replacing powers in RIPA 2000, section 8(4)). Part II chapter 1 of the Bill deals with targeted powers and replaces not only the Part I powers of RIPA but also those in the Wireless Telegraphy Act 2006. The main changes in the Bill relate to authorisation rather than the extent of the powers. The Bill will provide a new **'double-lock' authorisation procedure** whereby warrants are issued by a Secretary of State but must also be approved by a Judicial Commissioner before coming into force. Interception should not be undertaken if the information could be obtained by another less intrusive method. There is also some strengthening of the safeguards for especially sensitive intrusions. Thus, in addition to Judicial Commissioner approval, the Bill will include a requirement for the Prime Minister to be consulted before the Secretary of State can decide to issue a warrant to intercept an MP's communications. The Bill will set out details on the handling of intercept material to be included in codes of practice, including the special protections that apply to material that is legally privileged material or medical information.

613 Cm.9152, London, 2015. See also Dawson, J., *Draft Investigatory Powers Bill* (CBP-7371, House of Commons Library, 2015).

Bulk interception warrants under Part VI Chapter 1 allow for the collection of communications of persons who are outside the UK. A bulk interception warrant does not name or describe a person or premises as the subject of interception in the same way as a targeted interception warrant. These 'general warrants' were anathema to the common law but have long been promulgated by statute.[614] Whether the ECtHR will be so indulgent towards the proliferation of such indiscriminate powers remains to be seen, though recent indications suggest hostility.[615] Only the security and intelligence agencies may apply for a bulk interception warrant and only in relation to three statutory purposes: national security; prevention and detection of serious crime; and safeguarding the economic well-being of the UK as it pertains to national security. A bulk interception warrant must set out specific (albeit generic) purposes which must be met before any of the data that has been collected can be examined, as approved by a Secretary of State and Judicial Commissioners – an example is given of 'attack planning by ISIL in Syria against the UK'. Where a bulk warrant incidentally intercepts communications of persons who are in the UK, those communications may not be scrutinised unless an examination warrant has been obtained. **211**

Part III of the Bill replaces the existing framework on communications data by creating three categories of data: **'communications data'**, **'related communications data'**, and **'equipment data'**. 'Communications data' is data held by a CSP or available directly from the network which identifies a person or device on the network, and ensures that a communication reaches its intended destination, or describes how communications move across the network, or describes how a person has been using a service. It is in turn categorised into: entity data (data about entities or links between them but not including information about individual events; entities may be individuals, groups and objects such as mobile phones or other communications devices; and events data (which identifies or describes events consisting of one or more entities engaging in an activity at a specific point in time). **212**

'Related communications data' is data obtained **pursuant to an interception warrant**. Where it is not necessary to acquire the entire content of a communication the warrant may be limited to the acquisition of related communications data including certain information extracted from the content. 'Equipment data' is obtained under an equipment interference warrant (described below). Since communications data is meant to be distinct from content data (which can only be obtained under an intercept) the Bill creates a **new definition** of the 'content' of a communication or an item of information. The content of a communication or other item of private information is the data which reveals anything of what might be reasonably be expected to be the meaning of that data, disregarding any meaning that can be inferred from the fact of the communication or the existence of an item of private information. Whilst the Bill is clearer that RIPA on the meaning of communications data it has certainly not reduced the scope for intervention. Likewise, the Bill does not alter the basic scheme of agency self-authorisation. Thus, targeted communications data can be obtained on a case by case basis as authorised by a senior officer at a rank and in a public **213**

614 Compare *Entick v. Carrington* (1765) 95 ER 807; *Inland Revenue Commissioners v. Rossminster Ltd.* [1980] AC 952.

615 *Zakharov v Russia*, App. no.47143/06, 4 December 2015, paras.260, 264.

agency stipulated by Parliament. No judicial pre-authorisation or post-hoc scrutiny is required. Instead, **independent audit** of powers will be provided by the Investigatory Powers Commissioner (described below), very similar to the work of the Interception of Communications Commissioner's Office. The only new safeguard is that judicial approval will be demanded for requests by public authorities acquiring communications data to identify or confirm a journalistic source.

214 Instead of section 94 of the Telecommunications Act 1984, express powers are given to collect bulk communications data under Part VI Chapter 2. Access to large volumes of data is said to be essential to enable the identification of communications data that relates to subjects of interest and to piece together the fragments. Bulk communications data powers will be confined to the intelligence agencies for national security purposes. A **'double-lock' authorisation** procedure will be in place requiring warrants issued by a Secretary of State to be approved by a Judicial Commissioner before coming into force. Any interrogation of data will require a further warrant. Despite the wishes of the Anderson review, no compelling factual case is offered for these powers.

215 Data retention is dealt with in Part IV which requires Communications Service Providers to **retain customer data** for **up to 12 months**. The powers look much the same as in DRIPA, which may give rise to severe doubts about their legality under EU law. Indeed, the Bill goes further than prior law by requiring communications service providers to retain 'internet connection records' – a record of the internet services a device has accessed. At present, the Counter Terrorism and Security Act 2015, section 21, provides for the retention of data to resolve IP addresses. However, without the retention of ICRs, the task of resolving an IP address back to a single user will often not be possible as multiple users may be associated with a single IP address. Internet connection records (ICRs) are records of the internet services that have been accessed by a device at a particular time. The draft Bill will limit access to ICRs for one of three purposes: to identify the sender of a communication; to identify the communications services a person is using; to determine whether a person has been accessing or making available illegal material online. Though ICRs do not necessarily provide a full history of every web page that a person visited or every action carried out on that web page (because a full web address would be defined as content), there will be more information than about communications data by being able to identify a destination IP address which can often be resolved into a domain name.

216 Next, **equipment interference** is more fully set out and regulated than under section 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997. Part V will cover both targeted and bulk operations. It is arguable that bulk equipment interference was previously allowed, as the current legislation allows for warrants not only in respect of specified property but also specified 'wireless telegraphy'. Such operations may provide information that would otherwise be unobtainable, for example, by installing keystroke recognition software on a computer using encryption.

217 Targeted equipment interference is the power to invade equipment to obtain a variety of data, such as from computers or computer-like devices such as tablets, smart phones, cables, wires and switches. The interference can be carried out either remotely (such as through a virus) or by physically interacting

with equipment. Once again, the **powers are expanded** to some extent – in this case to the armed forces will also be able to apply for targeted equipment interference warrants to support military operations overseas. Thus, the security and intelligence agencies, armed forces and law enforcement agencies will be able to apply for an **Equipment Interference Warrant**. Equipment interference authorisations will be issued to law enforcement agencies by a Chief Constable and subsequently approved before coming into force by a Judicial Commissioner for the purpose of the prevention and detection of serious crime. The armed forces' warrants will be issued in the interests of national security by a Secretary of State and approved by an independent Judicial Commissioner. Security and intelligence agencies' warrants will be issued by a Secretary of State and subsequently approved by an independent Judicial Commissioner. A warrant can be applied for in the interests of national security, preventing and detecting serious crime, and in the interests of economic well-being (where they are also relevant to the interests of national security). Material derived from equipment interference may be used in evidence – only intercepts remain off limits to the courts.

Bulk equipment interference under Part VI Chapter 3 will allow agencies to **218**
capture large quantities of foreign-focused material which will then be processed. Access to this data is said to be crucial to discover new and emerging targets or to enable fragments of communications or other data relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

Warrants will be subject to the 'double-lock' authorisation procedure – issu- **219**
ance by a Secretary of State and approval by a Judicial Commissioner before coming into force. The material obtained through bulk EI can only be analysed if the reason for doing it relates to an operational purpose agreed at the time of the warrant. If the investigation requires that the data of someone in the UK needs to be examined, the agency must acquire a separate and additional targeted warrant from a Secretary of State and an independent Judicial Commissioner.

Next **bulk personal datasets ('BPDs')** are dealt with under Part VII, which **220**
provides more specific guidance than currently given under the general tasking powers of the Security Service Act 1989 and the Intelligence Services Act 1994 which were revealed for the first time as being used for this purpose in 2015. The agencies wish to acquire and use BPDs for several reasons: to help identify subjects of interest without the use of more intrusive techniques); to establish links between individuals and groups or to improve understanding of a target's behaviour and connections; and to verify information obtained through other sources. The Bill envisages two types of warrant: class warrants, covering particular types of BPDs such as travel data, driving licences, the electoral roll, and medical records where 'the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service';[616] and specific warrants, covering a specific dataset which will usually be held by a single data processor often in the private sector. Secretaries of State will issue warrants authorising the use of BPDs, and a Judicial Commissioner must approve the issuance.

616 Bill, cl. 150(1)(b).

221 The final aspect of the Bill, Part VIII, deals with **oversight**. As already indicated, the more intrusive powers in the Bill (warrants for interception, equipment interference by the security and intelligence agencies, and powers in bulk) will be overseen by **independent Judicial Commissioners** who will consider the justification for executive warrants on judicial review principles.[617] Judicial Commissioners will also approve the use of certain surveillance and equipment interference powers by law enforcement agencies. At the same time, full judicial pre-authorisation is not advanced by the Bill. In line with the views of the Intelligence and Security Committee, the Bill persists with most authorisations being issued by the Secretary of State. The justification is that the importance of executive authorisation in overseeing the use of intrusive powers and ensuring accountability to Parliament must remain predominant. By comparison, the Anderson Report recommended that Judicial Commissioners authorise almost all warrants, in line with current practice on approvals for police property interference, intrusive surveillance and long-term undercover operations, which require a Commissioner's approval under RIPA Part 2 powers. Exceptions would be allowed only for national security cases relating to foreign policy or defence and bulk warrants where the Secretary of State's decision would be subject to prior review by a Judicial Commissioner. This persistent faith in the empowerment of the executive is largely misplaced. Crown Ministers do not have the training or knowledge or time to make forensic decisions, whereas judges have shown an increasing ability to handle security matters.[618] The claim that political considerations and risks are in play is belied by the fact that the Ministers always refuse to discuss individual cases on security grounds.[619] If politicians are dissatisfied with how the judges handle security cases, then they can always say so in Parliament and seek to amend the law, but, as illustrated by the aftermath of the judicial condemnation of detention without trial, wiser heads either in Parliament or officialdom will usually see more sense in the deliberation of judges than the fulmination of inconvenienced politicians.[620]

222 The Judicial Commissioners will form part of a **new unified oversight body**, the **Investigatory Powers Commission ('IPC')**, which is promised significantly greater resources, including technical and legal resources. The IPC will oversee all investigatory powers: interception, communications data, equipment interference, the work of the agencies (as formerly overseen by the Intelligence Services Commissioner), bulk personal datasets, and the work of public authorities formerly overseen by the Chief Surveillance Commissioner.

223 Fewer changes await the **Investigatory Powers Tribunal ('IPT')**. The main change is to create a right to challenge the decisions of the IPT in a higher court within the UK rather than going directly to Strasbourg.[621]

---

617 Such principles are meant to confine the role of the judge but have not much constricted oversight in terrorism related cases: see Walker, C.P., *The Anti-Terrorism Legislation* (Third edition, Oxford University Press, Oxford, 2014) chap. 7.

618 See Walker, C., 'Terrorism prosecutions and the right to a fair trial' in Saul, B., (ed.), *Research Handbook On International Law And Terrorism* (Edward Elgar, Cheltenham, 2014).

619 For multiple examples, see House of Commons Public Administration Select Committee, *Ministerial Accountability and Parliamentary Questions* (2004–05 HC 449) vol. II.

620 For the debates around the decision in A v *Secretary of State for the Home Department* [2004] UKHL 56, see Walker, C., 'Prisoners of „war all the time"' [2005] *European Human Rights Law Review* 50.

621 As in *Kennedy v United Kingdom*, App. no.26839/05, 18 May 2010.

A complacently rosy picture is painted of the ISC, which therefore escapes any reform. In the view of the Home Office: **224**

'The ISC's powers were strengthened and it was given additional resources as a result of the Justice and Security Act 2013 and the preceding Green Paper on Justice and Security. Given these recent reforms, we do not think that further reform is necessary – the ISC's powerful reports into the post-Snowden 'Prism' allegation (July 2013); the Woolwich attack (November 2014) and Privacy and Security (March 2015) show that it has the necessary powers, resource and independence to provide robust Parliamentary oversight.'[622]

As mentioned earlier, debates on the Bill followed after the writing of this paper, and so no attempt will be made to give a comprehensive picture of the new legislation, not least because most provisions are still not yet in force. Nevertheless, it may be commented that opposition to the legislation was often focused on the issues of whether bulk collection powers were justifiable and proportionate and whether there was sufficiently strong oversight (especially judicial oversight) over their exercise. Some reassurance was gained on the first point from a further inquiry by **David Anderson, *Report of the Bulk Powers Review***.[623] The Investigatory Powers Act was finalised on the 29 November 2016. Compared to the designs set out by Anderson in his report, *A Question of Trust*, Anderson himself has expressed several misgivings regarding: the "dual lock" system for authorising interception warrants unnecessarily involves a government minister in the judicial function of warrant checking; whether advance safeguards on some of the new bulk powers such as large-scale "thematic" equipment interference or hacking are adequate, especially as they are granted to the police as well as the intelligence agencies; and the insufficient structural recognition and support for the Investigatory Powers Commission which in reality will extend to intelligence supervision beyond investigatory powers.[624] Most of the Investigatory Powers Act 2016 has not yet been brought into force, but the one notable exception concerns Part 4 of the 2016 Act relating to the retention of communications data, which was brought into force in late 2016; but the provisions of Part 4 requiring approval by the Investigatory Powers Commissioner of the decision of the Secretary of State to give or vary a retention notice or to review a retention notice have not yet commenced, as the Commissioner has not yet been appointed.[625] Any retention notice given or varied without the approval of the Commissioner ceases to have effect 3 months after the date on which the requirement for Commissioner approval comes into force. As a result of this commencement, sections 1 and 2 of the Data Retention and Investigatory Powers Act 2014 are repealed (subject to a transitional period of 6 months during which a retention notice given under the 2014 Act continues to have effect for a period of 6 months from the 30th December). This renewal of the UK's data retention legislation was timely because, just a few days later, the European Court of Justice in *Joined Cases C-203/15 and C-698/* **224a**

622 Home Office, *Investigatory Powers Bill: Factsheet: Oversight* (London, 2015).

623 (Cm.9326, London, 2016).

624 See https://terrorismlegislationreviewer.independent.gov.uk/the-investigatory-powers-act-2016-an-exercise-in-democracy/.

625 See Investigatory Powers Act 2016 (Commencement No. 1 and Transitional Provisions) Regulations 2016, SI 2016/1233.

15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson decided that the Data Retention and Investigatory Powers Act 2014 breached Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union. Whether the same fate would befall Part 4 of the Investigatory Powers Act 2016, which does contain some extra safeguards though by no means all those specified by the Court, remains for the future. Certainly, the Investigatory Powers Act 2016 is far from the final word on the subject, especially as the Brexit decision may allow for some extra flexibility in terms of the future legal regime for data protection.

G. Conclusions

225 Oversight and accountability for surveillance in the UK is of remarkably recent origin. The regulatory systems which are now in operation date largely from RIPA Act 2000, which has produced a complex, uneven, and bureaucratic landscape, perhaps reflecting British tradition for *ad hoc* solutions and organisational outgrowth and based on internal rather than external review.

226 This survey has next demonstrated a **growing acceptance**, increasingly impelled by human rights jurisprudence, that ‚[the] **trend towards legalism in the intelligence field is desirable**: law is a necessary condition for constitutionalism'.[626] At the same time, there are risks inherent in simplistically merging the standards set for intelligence in the security world and evidence in the legal world.[627] The safeguards of oversight and accountability for each should be carefully applied to ensure **fairness** and continued **effectiveness**. Delivery of these ideals to date is far from secure whether in terms of the standards of respect for individual rights set by the ECHR or the standards for democratic accountability set by the Venice Commission.[628] Too often, while surveillance techniques have been enshrined in law, the law has adopted an impoverished application of legal formality rather than more substantive oversight. The result is that campaigns against surveillance have become prominent, sparked not just by counter terrorism measures but also by more prevalent techniques such as CCTV and DNA sampling.[629]

626 Walker, C., 'Keeping control of terrorists without losing control of constitutionalism' (2007) 59 *Stanford Law Review* 1395, 1456.

627 Walker, C., 'Intelligence and Anti-terrorism Legislation' (2005) 44 *Crime, Law and Social Change* 387.

628 European Commission For Democracy Through Law (Venice Commission), *Report on the Democratic Oversight of the Security Services* (CDL-AD(2007)016, Strasbourg, 2007) and *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies* (CDL-AD(2015)006, Strasbourg, 2015).

629 See Information Commissioner, *A Report on the Surveillance Society* (Wilmslow: 2006); House of Commons Home Affairs Committee, *A Surveillance Society?* (2007–08 HC 58, and Government Reply, Cm.7449, London, 2008); House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State* (2008–09 HL 18, and Government Reply, Cm.7616, London, 2009).

Because of the foregoing trends, the intelligence agencies can expect in the future to have to contend with a **more stringent and judicialised legal environment**, though whether this emphasis on judges and tribunals wins the favour of the executive and Parliament, both of which savour their involvement with intelligence agencies, remains to be seen. Certainly, a more independent and pro-active form of accountability and oversight which perhaps reveals general issues for public debate might be beneficial and might also promote fairness and efficiency in the security and intelligence community in ways which better meet international expectations as to the observation of the rule of law even in this most challenging of state functions. **227**