National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

UNITED KINGDOM

Version of 25 September 2014

Human Rights Law Centre
University of Nottingham
Ian Brown

1 Surveillance legal framework

[1]. The UK's Government Communications Headquarters (GCHQ), alleged by Edward Snowden to be undertaking mass surveillance of online activities, operates under the Intelligence Services Act 1994.[1] GCHQ's first statutory function is "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" (s.3 (1)(a) Intelligence Services Act 1994).

[2]. GCHQ's Director must ensure "that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings" (s.4(2) ISA). These functions can be exercised 'in the interests of national security, the economic well-being of the UK,' and 'in support of the prevention or detection of serious crime' (s.3(2) ISA).

[3]. "National security" is a term that has been broadly interpreted in UK law. In a leading case, the Court of Appeal agreed with a government submission that it "is a protean concept, 'designed to encompass the many, varied and (it may be) unpredictable ways in which the security of the nation may best be promoted'."[2]

[4]. The key statute regulating interception of telecommunications is the Regulation of Investigatory Powers Act 2000 (RIPA – specifically, Part 1 Chapter 1),[3] as amended by the Data Retention and Investigatory Powers Act 2014.[4] GCHQ is understood to be exclusively responsible for large-scale interception, although a range of intelligence, policing and tax authorities (The Security Service, Secret Intelligence Service, GCHQ, National Crime Agency, Scottish Crime and Drug Enforcement Agency, Metropolitan Police, Royal Ulster Constabulary, any force maintained under s.1 of the Police (Scotland) Act 1967, Her Majesty's Revenues and Customs, Defence Intelligence, and the competent authority under any international mutual assistance agreement) may also apply to the Secretary of State (a senior government minister) for a warrant to intercept communications. It is the author's opinion that these bodies undoubtedly receive information obtained by GCHQ from its large-scale interception programmes revealed by Edward Snowden, although it may not be labelled as such.

[5]. All communications that begin and/or end outside the UK are "external" communications. These may be intercepted by GCHQ under a warrant issued by the Secretary of State under s.8(4) RIPA, specifying the facilities affected (such as the fibre optic cables landing in the UK that carry much of the Internet traffic between continental Europe and the USA), and certificates issued by the Secretary of State specifying the types of material that can be accessed from this intercepted material.[5] It has been reported that ten "basic" certificates exist, covering broad categories of data such as "fraud, drug trafficking and terrorism". The warrants must be renewed every six months (three where they relate to preventing or detecting serious crime).

---

[1] United Kingdom, Parliament (2004) Intelligence Services Act 2004, available at: www.legislation.gov.uk/ukpga/1994/13/contents.
[2] United Kingdom, Court of Appeal (2003) *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153.
[3] United Kingdom, Parliament (2000) Regulation of Investigatory Powers Act 2000, available at: www.legislation.gov.uk/ukpga/2000/23/contents.
[4] United Kingdom, Parliament (2014) Data Retention and Investigatory Powers Act 2014, available at: www.legislation.gov.uk/ukpga/2014/27/contents/enacted.
[5] United Kingdom, The Guardian (2013) The Legal Loopholes that allow GCHQ to spy on the world, 21 June 2013, available at: www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

[6]. Postal and telecommunications service providers may intercept communications "for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services" (RIPA s.3).

[7]. A second key power is contained in the Telecommunications Act 1984:[6]

> *94 Directions in the interests of national security etc.*
>
> *(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom…*
>
> *(8) This section applies to OFCOM and to providers of public electronic communications networks.*

[8]. Very little is known about the use of this broad power. The Interception of Communications and Intelligence Services Commissioners appointed under RIPA have both told the UK Parliament they do not oversee its use.[7]

[9]. Under the Data Retention and Investigatory Powers Act 2014 and the Data Retention Regulations 2014,[8] public telecommunications operators notified by the Secretary of State are required to retain for up to 12 months certain data generated or processed in the UK relating to telephony and Internet communications. "Communications data" (or "metadata" as it is called in the US) – information about subscribers and their use of a communications service – is collected by many government agencies from UK Communications Service Providers using powers in Part 1 Chapter 2 of RIPA.

[10]. In relation to gaining unauthorised access to computer networks and systems outside the UK, the Intelligence Services Act 1994 provides:

> *7 Authorisation of acts outside the British Islands.*
>
> *(1) If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section…*
>
> *(9) For the purposes of this section the reference in subsection (1) to an act done outside the British Islands includes a reference to any act which—*
>
> *(a) is done in the British Islands; but*

[6] United Kingdom, Parliament (1984) Telecommunications Act 1984, available at: www.legislation.gov.uk/ukpga/1984/12/contents.
[7] Home Affairs Committee – Seventeenth Report, Counter-Terrorism, 30 April 2014, §175, available at: www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm.
[8] United Kingdom, Parliament (2014) The Data Retention Regulations 2014, available at www.legislation.gov.uk/uksi/2014/2042/contents/made.

(b) is or is intended to be done in relation to apparatus that is believed to be outside the British Islands, or in relation to anything appearing to originate from such apparatus.[9]

[11]. While the smaller governing coalition party (the Liberal Democrats) and the main opposition party (Labour) have both called for surveillance law reform, the current government (in power until May 2015) has made no public plans to do so. Labour and the Liberal Democrats want stronger oversight by converting the existing interception and intelligence commissioners - retired judges - whose work is largely unknown by the public, into a higher-profile Inspector General. And both argue that the Regulation of Investigatory Powers Act now needs changing, in areas such as stronger safeguards for "metadata", and looking again at the broad powers given for GCHQ surveillance of "external" communications that start and/or end outside the British Isles (i.e. most Internet communications).[10]

[12]. The Independent Reviewer of Terrorism Legislation, appointed by the Secretary of State under section 36(1) of the Terrorism Act 2006,[11] is conducting a review (required by the Data Retention and Investigatory Powers Act 2014 s.7) of "the operation and regulation of investigatory powers," and is required to report by 1 May 2015. The government elected in May 2015 is expected to act on his recommendations.

2 Privacy safeguards

[13]. The Secretary of State must put in place "general safeguards" in relation to intercepted material and related communications data (s.15(2) RIPA) to ensure:

(a) the number of persons to whom any of the material or data is disclosed or otherwise made available,

(b) the extent to which any of the material or data is disclosed or otherwise made available,

(c) the extent to which any of the material or data is copied, and

(d) the number of copies that are made,

is limited to the minimum that is necessary for the authorised purposes.[12]

[14]. This material must be stored in a "secure manner" and "destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes." Such protections must also be in place when material is "surrendered to authorities of a country or territory outside the United Kingdom". However, there are no further statutory controls on the sharing of such data with foreign governments.

[9] United Kingdom, Parliament (2004) Intelligence Services Act 2004, section 7, available at: www.legislation.gov.uk/ukpga/1994/13/section/7.
[10] United Kingdom, Ian Brown (2014) Finally, some high-level UK debate on Internet surveillance, available at: http://doooooooom.blogspot.co.uk/2014/03/finally-some-high-level-uk-debate-on.html.
[11] United Kingdom, Parliament (2006) Terrorism Act 2006, section 36(1), available at: www.legislation.gov.uk/ukpga/2006/11/section/36.
[12] United Kingdom, Parliament (2000) Regulation of Investigatory Powers Act 2000, section 15(2), available at: www.legislation.gov.uk/ukpga/2000/23/section/15.

[15]. The Secretary of State must issue codes of practice on interception and the acquisition and disclosure of communications data, but these provide little additional detail to the protections set out in s.15 of RIPA.

[16]. The Human Rights Act 1998 requires public authorities to act in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, including Art. 8.

[17]. Two Commissioners (who hold or have held high judicial office) are appointed by the Prime Minister to oversee the use of RIPA powers: the Intelligence Services Commissioner, and the Interception of Communications Commissioner. Both must provide reports to the Prime Minister (the former annually, the latter every six months), who may redact sensitive information before they are provided to Parliament.

[18]. The Justice and Security Act 2013 established an Intelligence and Security Committee of Parliament to oversee the intelligence agencies. The members must be nominated by the Prime Minister, who may also redact its annual report.[13]

[19]. The Data Protection Act 1998 implements the EU Data Protection Directive (95/46/EC). However, s.28 contains a broad exemption for national security purposes:

> *(1) Personal data are exempt from any of the provisions of—*
>
> *(a) the data protection principles,*
>
> *(b) Parts II, III and V, and*
>
> *(c) sections 54A and 55,*
>
> *if the exemption from that provision is required for the purpose of safeguarding national security…*[14]

3 Judicial or non-judicial remedies

[20]. The UK does not have a codified constitution that would allow a constitutional challenge to government surveillance.

[21]. The European Convention on Human Rights' protections can be directly enforced by UK courts under the Human Rights Act 1998, and those courts must take notice of – but are not bound by – the jurisprudence of the European Court of Human Rights.[15] The senior courts may make a Declaration of Incompatibility that declares that a UK legislative provision is not in accordance with the Convention, but it is then for Parliament to decide whether to change the law to remedy this incompatibility. Until this happens, the provision remains in effect.[16]

---

[13] United Kingdom, Parliament (2013) Justice and Security Act 2013, available at: www.legislation.gov.uk/ukpga/2013/18/contents/enacted.
[14] United Kingdom, Parliament (1998) Data Protection Act 1998, section 28, available at: www.legislation.gov.uk/ukpga/1998/29/section/28.
[15] United Kingdom, Parliament (1998) Human Rights Act 1998, available at: www.legislation.gov.uk/ukpga/1998/42/contents.
[16] United Kingdom, Parliament (1998) Human Rights Act 1998, section 4, available at: www.legislation.gov.uk/ukpga/1998/42/section/4.

[22]. The Investigatory Powers Tribunal (IPT), established by RIPA, has exclusive jurisdiction to hear complaints about the intelligence agencies or interception.[17] However, since there is no statutory provision for individuals to be notified that they have been the subject of interception or other surveillance, they have little opportunity to contest it. Intercepted material may not be introduced in legal proceedings outside the Tribunal or a limited range of other special proceedings (ss.17-18 RIPA).[18]

[23]. A Pakistani human rights group, Bytes for All, has filed suit with the IPT. Their complaint alleges that GCHQ's mass surveillance programme infringes their rights under ECHR Articles 8, 10 and also 14, given the discriminatory effect of GCHQ's focus on non-UK communications.[19] An initial directions hearing combined this complaint with four others, filed by Privacy International, Amnesty International, Liberty, the American Civil Liberties Union and others, and a first hearing was held the week of 14 July 2014.

[24]. In a second case at the IPT, the government's lawyers have given assurances that they will not make use of any intercepted material between the two complainants, Belhaj and Bouchar, and their UK lawyers, who are bringing a case against the UK government for complicity in torture.[20]

[25]. The IPT is not one of the "senior courts" that under the Human Rights Act may make a declaration of incompatibility of UK law with the ECHR. It has no duty to publish any details of its negative decisions. Nor may decisions be appealed. Up until December 2012, the IPT upheld 10 out of 1469 complaints.[21]

[26]. Three UK-based organisations (Big Brother Watch, Open Rights Group and English PEN) and a Berlin-based academic (Dr. Constanze Kurz) have complained directly to the European Court of Human Rights about the infringement of their privacy. They argue that the UK courts cannot provide an effective remedy under the Convention, and that they therefore do not need to first exhaust domestic remedies. The European Court has prioritised the application, but stayed it until the conclusion of the IPT case described above.[22]

---

[17] United Kingdom, Parliament (2000) Regulation of Investigatory Powers Act 2000, section 65-70, available at: www.legislation.gov.uk/ukpga/2000/23/section/65.

[18] United Kingdom, Parliament (2000) Regulation of Investigatory Powers Act 2000, section 17-18, available at: www.legislation.gov.uk/ukpga/2000/23/section/17.

[19] United Kingdom, Investigatory Powers Tribunal (2014) *Bytes for All v The Secretary of State for Foreign and Commonwealth Affairs and others*, available at: www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ipt-bytes-for-all.pdf.

[20] United Kingdom, The Guardian (2014) Ian Cobain and Owen Bowcott, Spy agency lawyers agree not to read intercepted emails on torture case, 30 January 2014, at www.theguardian.com/uk-news/2014/jan/30/spy-agency-lawyers-emails-libyan-torture-uk.

[21] United Kingdom, Parliament (2009) Hansard HC Debates, 23 April 2009: Column 858W, available at: www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090423/text/90423w0016.htm#column_858W; United Kingdom, Parliament (2010) Hansard HC Debates, 11 January 2010: Column 701W, available at: www.publications.parliament.uk/pa/cm200910/cmhansrd/cm100111/text/100111w0013.htm#column_701W; United Kingdom, Interception of Communications Commissioner's Office (2010), Annual Report of the Interception of Communications Commissioner for 2010, page 54, available at: www.iocco-uk.info/docs/2010%20Annual%20Report.pdf; United Kingdom, Intelligence Services Commissioner's Office (2010), Report of the Intelligence Services Commissioner for 2010, page 16, available at: http://isc.intelligencecommissioners.com/docs/Report%20of%20the%20Intelligence%20Services%20Commissioner%20for%202010.pdf.

[22] United Kingdom, European Court of Human Rights (2014) *Big Brother Watch and others v the United Kingdom*, Application No. 58170/13 §§62-66, available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713 - {"itemid":["001-140713"]}.

Annex 1 – Legal Framework relating to mass surveillance

A. Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Regulation of Investigatory Powers Act 2000 (Public General Act of Parliament) Part 1 Chapter 1, as amended by the Data Retention and Investigatory Powers Act 2014 (Public General Act of Parliament)	Any individual – limits are on geographical extent(communications begin and/or end outside the British Isles) of communications (s.8(5)(a)), or location of targeted individual (who is known to be for the time being in the British Islands)(s.16(2)).	Information sought cannot "reasonably be obtained by other means" (s.5(4)) Conduct is "proportionate to what is sought to be achieved" (s.5(2)(b)).	s.5(3) "necessary— (a) in the interests of national security; or (b) for the purpose of preventing or detecting serious crime; or (c) for the purpose of safeguarding the economic well-being of the United Kingdom, in circumstances appearing to the Secretary of State	Secretary of State (a senior government minister, usually the Foreign Secretary) must issue and renew interception warrants. Section 8(1) warrants are not "mass" – they name an individual or premises in the UK. Secretary of State must issue certificates describing the "intercepted material the	Interception warrant is applied for by an intelligence agency head, chief constable of police, or head of tax authority. Warrant is issued/renewed by Secretary of State or (in urgent situations, and for a limited time period only) a senior official. Intercepted material may be examined for purposes certified as necessary by the Secretary of State.	The law allows untargeted interception of any communications that begin and/or end outside the British Islands (s.8(4)). The following must be limited "to the minimum that is necessary for the authorised purposes": "(a) the number of persons to whom any of the material or data	The law allows untargeted interception of any communications that begin and/or end outside the British Islands (s.8(4)), and examination of that intercepted material certified by the Secretary of State to fall within the purposes of national security, preventing or detecting serious crime, or

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			to be relevant to the interests of national security"	examination of which he considers necessary" (s.8(4)). Warrants and certificates may be modified "at any time" (s.10(1)) by the Secretary of State. A senior official may modify a certificate where he is expressly authorized to do so by the certificate.	The Secretary of State must make arrangements as he considers "necessary" to ensure intercepted material is retained "in a secure manner" (s.15(5)). Each copy of intercepted material must be "destroyed as soon as there are no longer any grounds for retaining it" (s.15(3)).	is disclosed or otherwise made available, (b) the extent to which any of the material or data is disclosed or otherwise made available, (c) the extent to which any of the material or data is copied, and (d) the number of copies that are made" (s.15(2)). Warrants are valid for a period of six months (for national security or economic wellbeing of UK)	protecting the economic well-being of the UK. Interception warrants may be served "on a person outside the United Kingdom (and may relate to conduct outside the United Kingdom)".

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
						or three months (preventing or detecting serious crime) (s.9(6)). Warrants should be cancelled when no longer necessary (s.9(3)).	
Telecommunications Act 1984 s.94	Any	When it is "in the interests of national security or relations with the government of a country or territory outside the United Kingdom", and the Secretary of State "believes that the conduct required by the direction is	Not specified in Act	Directions can be given by the Secretary of State, of a general or particular character	None specified in the Act	None	Yes

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
		proportionate to what is sought to be achieved"					

B. Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
The Human Rights Act 1998 incorporates the European Convention on Human Rights into domestic law.	Right to Respect for Private life, home and correspondence: Article 8 of the ECHR.	To all individuals within the UK's jurisdiction. The Investigatory Powers Tribunal has accepted claims from persons outside the UK.	To all acts of the UK government.
The Data Protection Act 1998 transposes the EU Data Protection Directive (95/46/EC) into domestic law; but personal data are exempt from almost the whole Act when required for the purposes of "safeguarding national security" (as certified by a government minister)			
The Regulation of Investigatory Powers Act 2000 s.15 includes privacy protections against surveillance, as descibed in the previous table			
The European Communities Act 1972 gives effect to EU "rights, powers, liabilities, obligations and restrictions from time to time created or arising by or under the Treaties" – including (to a contested extent) the Charter of Fundamental	Articles 7 and 8 of the Charter of Fundamental Rights, so far as as the UK is acting within the fields of EU law. This is strongly constrained in relation to national security mass surveillance by Article 4(2) of the Treaty on European Union. Such surveillance can also take place for the purposes of preventing and detecting serious crime, and protecting the economic well-being of the UK, although the government has argued the initial interception is for national security purposes	The Charter applies as far as the UK is implementing EU law – for example, on data retention – but not otherwise (e.g. national security interception).	This needs to be clarified by the Court of Justice of the EU, but general principles suggest that whenever EU law is being applied, by the Union or the Member States, the Charter applies regardless of territoriality.

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	List specific privacy and data protection safeguards put in place by this law(s)	Indicate whether rules on protection of privacy and data protection apply: only to nationals or also to EU citizens and/or third country nationals	Indicate whether rules on protection of privacy and data protection apply: only inside the country, or also outside (including differentiation if EU or outside EU)
Rights, despite Protocol 30 to the Treaty of Lisbon.	regardless. These further purposes are also covered (less emphatically) by TEU Art. 4(2).		
Data Retention and Investigatory Powers Act 2014	Section 7 requires that "The Secretary of State must appoint the independent reviewer of terrorism legislation to review the operation and regulation of investigatory powers…before 1 May 2015."	N/A	N/A

Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Interception of Communications Commissioner	(Retired) judge appointed by and reporting to the Prime Minister (hence executive)	Regulation of Investigatory Powers Act 2000 s.57	Ex post, ongoing, with annual report	Commissioner (appointed by Prime Minister) directly oversees interception with chief inspector; has nine inspectors to oversee use of communications data and prison interception, and two office staff.	Obtain "documents and information as he may require" from officials and affected businesses involved in communications surveillance. Keep under review the exercise and performance of: (i) the Secretary of State "relating to the granting and operation of interception warrants"; and (ii) persons who have powers and duties "relating to the acquisition and disclosure of communication data". Keep under review "the adequacy of arrangements for safeguards relating to use that is made of interception material". Half-yearly reporting obligation to Prime Minister.
Intelligence Services Commissioner	(Retired) judge appointed by and reporting to the Prime Minister (hence executive)	Regulation of Investigatory Powers Act 2000 s.59	Ex post, ongoing, with annual report	Appointed by Prime Minister. Part-time, with a part-time secretary.	Obtain "documents and information as he may require" from officials. Ensure that "warrants for entry on to, or interference with, property (or with wireless telegraphy)" and "authorisations for acts done outside the United Kingdom" issued by the Secretary of State are in accordance with the law. Oversee the Secretary of State's powers and duties in the granting of authorisations for "intrusive surveillance and the investigation of electronic data protected

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
					by encryption". Oversee the authorisation of "directed surveillance", "the conduct and use of covert human intelligence sources (CHIS)" and "the investigation of electronic data protected by encryption" granted by members of the intelligence services, Ministry of Defence Officials and members of the armed forces. Keep under review the adequacy of the safeguards laid out in Part III of the Regulation of Investigatory Procedures Act 2000 relating to such persons. On direction from the Prime Minister review "any other aspects of the functions [of such persons] engaging in intelligence activities (excepting interception of communications)". Assist the Investigatory Powers Tribunal when required. Consulting with the Home Office to advise on the propriety of extending the regime established by the Terrorism Prevention and Investigation Measures Act 2011. Annual reporting obligation to Prime Minister.

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
Intelligence and Security Committee	Statutory Parliamentary committee	Justice and Security Act 2013 Part 1 and Schedule 1	Ex post, ongoing	Nine Members of Parliament/Peers (not Ministers) nominated by Prime Minister and elected by House of Commons/Lords for each Parliament. Committee has a General Investigator, a Secretariat of seconded civil servants, and may obtain independent legal advice from the Treasury Solicitor and financial expertise from the National Audit Office. The budgets of the intelligence agencies are reviewed by the chair of the Public Accounts Committee.	Oversees "expenditure, administration, policy and operations" of agencies (but not on-ongoing operations, except as requested by Prime Minister or volunteered by intelligence agencies or government departments), and other activies set out in a (published) Memorandum of Understanding with the Prime Minister. Reports annually and as appropriate to Parliament, but must exclude matters that Prime Minister considers are "prejudicial to continued discharge of functions" of agencies. May obtain information from agencies and government departments, except where Secretary of State blocks disclosure of "sensitive" information, including that provided by foreign governments.

Annex 3 – Remedies

Regulation of Investigatory Powers Act 2000; Data Protection Act 1998; Human Rights Act 1998				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
Collection **Analysis** **Storing** **Destruction** **After the whole surveillance process has ended**	The subject will only be informed if if they can convince the Information Tribunal a national security certificate was wrongly issued,[23] or successfully complain to the Investigatory Powers Tribunal and persuade them to order this access.	Only if they can convince the Information Tribunal a national security certificate was wrongly issued, or successfully complain to the Investigatory Powers Tribunal and persuade them to order this access.	Complaints about interception or activities of intelligence agencies must be made to the quasi-judicial Investigatory Powers Tribunal established under the Regulation of Investigatory Powers Act. The IPT only found in favour of 0.75% of complainants from 2001-2012. A small number of rulings have been published.[24]	Data Protection Act rights violated (almost unheard of). Regulation of Investigatory Powers Act incompatible with ECHR (claims currently before IPT and ECtHR). RIPA provisions breached. Private sector organisation supplies personal data to government in breach of contractual obligations. Government obtains personal data from private sector organisation outside statutory framework (and hence in breach of ECHR if there is no law legitimising the interference).

[23] United Kingdom, Chris Pounder (2014) Should national security certificates exclude the Data Protection Principles? *Hawktalk*, 6 February 2014, available at http://amberhawk.typepad.com/amberhawk/2014/02/should-national-security-certificates-exclude-the-data-protection-principles.html

[24] United Kingdom, Investigatory Powers Tribunal (2014) Key IPT Rulings, available at: www.ipt-uk.com/sections.asp?pageID=73&sectionID=19&type=rulings.

Annex 4 – Surveillance-related case law at national level

The Investigatory Powers Tribunal, which has exclusive jurisdiction to hear claims relating to interception and the conduct of the intelligence agencies, rarely publishes its decisions. The following are the only two relevant judgments published. Cases against the UK at the European Court of Human Rights (such as *Kennedy v UK* and *Liberty v UK*) are a better guide to the government's position, and to its compatibility with the Convention.

Case title	*The British-Irish Rights Watch and others v Security Service, Government Communications Headquarters and the Secret Intelligence Service*
Decision date	9 December 2004
Reference details	Investigatory Powers Tribunal Decision IPT/01/77 - Rulings on Preliminary Issue of Law, at http://www.ipt-uk.com/docs/No%20IPT-01-77.pdf
Key facts of the case	Alleged infringement of privacy (Article 8) of complainants by the UK intelligence agencies, using a Regulation of Investigatory Powers Act 2000 s.8(4) untargeted warrant against "external" communications. It was contested that the accessing of the information obtained had not been in accordance with law as it had not been accessible or foreseeable that such a warrant would be issued.
Main reasoning/argumentation	Section 8(4) warrants do not name targets, and there are no published (accessible or foreseeable) criteria by which individuals' communications are identified for further examination; hence the intrusion is not in accordance with the law This requires i) the interference must have some basis in domestic law ii) it must be adequately accessible and iii) it must be formulated so that it is sufficiently foreseeable. The complainants relied upon the interpretation of in accordance with the law as outlined by the European Court of Human Rights in Valenzuela Contreras v Spain [1998] 28 EHRR 483 at 503 at paragraph 46.
Key issues (concepts, interpretations) clarified by the case	While greater quantities of communications may be intercepted under s.8(4) warrants, care must be taken by intelligence agencies over the necessity and proportionality of accessing specific communications from that large quantity. The tribunal held that the case law of the European Court of Human Rights cited by the complaints is not "clear and constant jurisprudence". Rather, the judgements of the European Court of Human Rights in Malone v UK, Klass v Germany, and Christie v UK are

	more representative of the interpretation of in accordance with the law and as such should be followed.
Results (sanctions) and key consequences or implications of the case	The tribunal held that the provisions regarding the right to intercept and access material covered by the section 8(4) warrant and the criteria by reference to which it is exercises are sufficiently accessible and foreseeable to be in according with law. The tribunal held that there are sufficient safeguards to ensure the foreseeability and accessibility of the warrants. The publication of selection criteria would be "risky and pointless" and "it is not part of the requirements for accessibility or foreseeability that the precise details of…safeguards should be published". In addition to this the Human Rights Act 1998 article 6(1) (requiring "public authorities to act compatibly with Convention rights") adds a further safeguard to RIPA. The tribunal followed the approach adopted in Christie v UK ECtHR whereby the court held that; "taking into account both the necessary narrow approach to Article 8(2) and the fact that the burden is placed upon the Respondent [to establish that the accessing of information obtained pursuant to a s8(4) warrant falls within the exception of in accordance with law as set out in article 8(2)], we are satisfied that the balance is properly struck."

Case title	*B v Security Service*
Decision date	31 March 2004
Reference details	Investigatory Powers Tribunal Decision IPT/03/01/CH - Rulings on Preliminary Issue of Law http://www.ipt-uk.com/docs/IPT_03_01_CH.pdf
Key facts of the case	The Claimant, a Member of Parliament, wanted to know whether the Security Service held personal data about him. After succeeding in having a blanket Data Protection Act national security certificate quashed by the Information Tribunal, the government disclosed some information held, but issued a new national security certificate and refused to confirm or deny whether further personal data was held. The claim is that this was irrational, unlawful and incompatible with Article 8 ECHR.
Main reasoning/argumentation	The Government argued that secrecy is essential to the work of Security Service, and the Neither Confirm Nor Deny policy is essential to preserve that secrecy. The claimant argued that Klass v Germany is authority for the fact that interference with Article 8(1) rights must not always be proven for an Article 8(2) justification to be required.
Key issues (concepts, interpretations) clarified by the case	Because the Tribunal has "extraordinary" powers to determine matters of fact about the intelligence agencies, it is distinguished from precedent regarding other courts and tribunals. The parties agreed it is for the Tribunal to determine in private whether any personal data is held on the complainant, and whether refusing to confirm or deny that fact interferes with his Article 8 rights, but disagreed in the intensity of the review required.
Results (sanctions) and key consequences or implications of the case	A "neither confirm nor deny" response does not interfere with Article 8(1) rights, even if it disturbs a complainant's everyday life or state of mind (citing Zehnalova v Czech Republic ECtHR, 14 May 2002 at 12). If personal data is held, the intelligence agency must "satisfy the Tribunal its conduct is not arbitrary, but rational and proportionate." If is not, the standard is "simply of judicial review on rationality principles."

Case title	*Belhaj and others v (1) Security Service (2) Secret Intelligence Service (3) Government Communication Headquarters (3) Government Communication Headquarters (4) Secretary of State for the Home Department (5)Secretary of State for Foreign and Commonwealth Affairs*
Date of interim decision	7 February 2014
Reference details	Investigatory Powers Tribunal at: http://www.ipt-uk.com/docs/IPT_13_132-9_H.PDF The Guardian at: http://www.theguardian.com/uk-news/2014/jan/30/spy-agency-lawyers-emails-libyan-torture-uk
Key facts of the case	Alleged breaches of the claimants' right to a fair trial (Article 6) and privacy (Article 8) due to the alleged interception of their legally privileged communications by the UK Government against whom the claimants were bringing a separate civil suit against for complicity in torture. Additionally a violation of Article 14 was alleged due to the discriminatory nature of the application of the interception.
Main reasoning/argumentation	Information not available.
Key issues (concepts, interpretations) clarified by the case	Both parties agreed on the applicability of the common law principle set out in Stiedl v Enyo Law [2011] EWHC 2649 (Comm) whereby, first, a court must consider whether there is a real risk that privileged material will give an advantage to the receiver or cause a disadvantage for the owner of the privileged information and, secondly, a court must conduct a balancing exercise to assess and then consider the appropriate relief, which may be either that the receiver of the information can no longer act as counsel or that the privileged information may not be made use of. As a result assurances were given by the respondents that intercepted privileged communications would not be made use of. Whilst accepting that the Stiedl v Enyo Law principle should be applied, the respondents undertook to communicate in closed hearing any information that a policy officer working

	on the claimants' case had read or listened to any of the claimants' legally privileged materials and seek the Tribunal's directions in closed hearing. This undertaking was accepted by the Tribunal at an interim hearing as it provided proper protection for the claimants.
Results (sanctions) and key consequences or implications of the case	Only documentation from the interim hearing has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.

Case title	*Privacy International v (1) Secretary of State for the Foreign and Commonwealth Affairs (2) The Secretary of State for the Home Department (3) The Secret Intelligence Service (5) Government Communication Headquarters (6) The Attorney General*
Date of hearing	14 July 2014 (conjoined hearing along with *Bytes for All v 1) Secretary of State for the Foreign and Commonwealth Affairs (2) The Secretary of State for the Home Department (3) The Secret Intelligence Service (5) Government Communication Headquarters (6) The Attorney General*)
Reference details	Privacy International at: https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy_international_ipt_grounds.pdf
Key facts of the case	Alleged interference with both the claimants' right to privacy (Article 8) and freedom of expression (Article 10) by the UK intelligence through their surveillance activities.

Main reasoning/argumentation	The claimants' contested that there rights had been interfered with on two grounds. Under Ground One it was contested that the distinction between "internal" and "external" surveillance made under the Regulation of Investigatory Powers Act 2000 resulted in there being no sufficiently clear legal regime protecting communications that are either sent or received outside of the British Islands. Under Ground Two it was contested that the blanket surveillance and mass collection of data under an intelligence operation known as Tempora (authorised by a Regulation of Investigatory Powers Act 2000 s.8(4) certified warrant) is not prescribed by law as the Regulation of Investigatory Powers Act 2000 does not provide sufficiently specific and or clear authorisation for such interception of communications. Furthermore it was contested that it cannot be justified as a proportionate response to a legitimate aim. In addition as a s.8(4) warrant only applies to "external communications" it was contested that it is likely that the operation will disproportionately affect non-UK citizens and is therefore in breach of Article 14 prohibiting discrimination. Argumentation put forward by the Respondent is unavailable as no hearing documentation has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.
Key issues (concepts, interpretations) clarified by the case	No hearing documentation has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.
Results (sanctions) and key consequences or implications of the case	No hearing documentation has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.

Case title	*Bytes for All v 1) Secretary of State for the Foreign and Commonwealth Affairs (2) The Secretary of State for the Home Department (3) The Secret Intelligence Service (5) Government Communication Headquarters (6) The Attorney General*
Date of hearing	14 July 2014 (conjoined hearing along with *Privacy International v (1) Secretary of State for the Foreign and Commonwealth Affairs (2) The Secretary of State for the Home Department (3) The Secret Intelligence Service (5) Government Communication Headquarters (6) The Attorney General*)
Reference details	Privacy International at: www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ipt-bytes-for-all.pdf.
Key facts of the case	Alleged infringement of the claimants' privacy (Article 8) and freedom of expression (Article 10) by the UK's mass surveillance activities. Following the Snowden revelations the UK authorities were found to be intercepting communications routed into, out or through the UK and subsequently storing and accessing a substancial portion of the data. These activities were authorised using s.8(4) Regulation of Investigatory Powers Act 2000 certified warrants that were being renewed on a rolling basis by the Secretary of State.
Main reasoning/argumentation	It was contested by the claimants' that in the absence of a clear legal framework governing such serveillance activities they are in breach of Article 8 as they are not proscribed by law. In addition it was contested that such practices are not a proportionate response to a legitimate aim and that the absence of judicial oversight over and rolling renewal of s.8(4) warrants is unjustified and disproportionate. The scale, selection and content of the search terms used to filter the material intercepted and the permission given to the US National Security Agency to select terms, along with the storage of data of individuals where there is no reason to suspect involvement in serious crime or terrorism were also contested to be unjustified and disproportionate. The claimants also asserted that a number of sections of the Regulation of Investigatory Powers Act 2000, including s.20, result in a disproportionate effect on non-UK nationals

	who are more likely to have their communications intercepted and thus constitute a breach of Article 14 ECHR (prohibition of discrimination). Argumentation put forward by the Respondent is unavailable as no hearing documentation has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.
Key issues (concepts, interpretations) clarified by the case	No hearing documentation has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.
Results (sanctions) and key consequences or implications of the case	No hearing documentation has been made public by the Investigatory Powers Tribunal http://www.ipt-uk.com/section.aspx?pageid=8, this was the position as of Thursday 25 September 2014.

Annex 5 – Key stakeholders at national level

Name of stakeholder	Type of stakeholder	Contact details	Website
GCHQ	Public authority	GCHQ, Hubble Road, Cheltenham, GL51 0EX. Email: pressoffice@gchq.gsi.gov.uk Telephone: 01242 221491	http://www.gchq.gov.uk/Pages/homepage.aspx
Cabinet Office	Government	70 Whitehall, London SW1A 2AS Telephone: 020 7276 3000	https://www.gov.uk/government/organisations/cabinet-office
Home Office	Government	Direct communications unit 2 Marsham Street London SW1P 4DF Email: public.enquiries@homeoffice.gsi.gov.uk Telephone: 020 7035 4848	https://www.gov.uk/government/organisations/home-office
Foreign and Commonwealth Office	Government	King Charles St, London SW1A 2AH. Email: fcocorrespondence@fco.gov.uk Telephone: 020 7008 1500	https://www.gov.uk/government/organisations/foreign-commonwealth-office
Privacy International	Civil society	62 Britton Street, London, EC1M 5UY. Email: INFO@PRIVACY.ORG Telephone: +44 (0) 20 3422 4321,	https://www.privacyinternational.org/
Liberty	Civil society	Liberty House, 26-30 Strutton Ground, London, SW1P 2HR. Telephone: 020 7403 3888.	http://www.liberty-human-rights.org.uk/
Open Rights Group	Civil society	Open Rights Group, Langdale House, 11 Marshalsea Road, London SE1 1EN Telephone: +44 (0)20 7096 1079	https://www.openrightsgroup.org/

		Email: info@openrightsgroup.org	
Big Brother Watch	Civil society	Big Brother Watch, 55 Tufton Street, London SW1P 3QL. Email: info@bigbrotherwatch.org.uk Telephone: +44 (0) 207 340 6030	http://www.bigbrotherwatch.org.uk/
Foundation for Information Policy Research	Civil society	Foundation for Information Policy Research, 10 Water End, Wrestlingworth, Sandy, Beds. SG19 2HA Telephone: +44 1223 334733 Email: chair2006@fipr.org	http://www.fipr.org/
Royal United Services Institute	Civil society	Royal United Services Institute for Defence and Security Studies, Whitehall, London, SW1A 2ET. Telephone: +44 (0)20 7747 2600	https://www.rusi.org/
Investigatory Powers Tribunal	Courts	The Investigatory Powers Tribunal, PO Box 33220, London SW1H 9ZQ. Telephone: 0207 035 3711	http://www.ipt-uk.com/
Intelligence and Security Committee	Parliament	Intelligence and Security Committee, 35 Great Smith Street, London SW1P 3BQ. Email: committee@isc.x.gsi.gov.uk	http://isc.independent.gov.uk/

Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources** ***(in accordance with FRA style guide)****:*

Government/ministries/public authorities in charge of surveillance

Home Affairs Committee Seventeenth Report, Counter-Terrorism, ordered by the House of Commons to be printed 30 April 2014.[25]

Main findings: "We have consistently been denied the opportunity to take evidence from senior officials who work in the national security structure and we are highly unimpressed that we had to summon the independent Intelligence Services Commissioner in order to take evidence from him… We do not believe the current system of oversight is effective and we have 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… We recommend that the if the Investigatory Powers Tribunal are unwilling to voluntarily produce a detailed annual report on their work, that legislation be amended so that they are required to do so… It is unacceptable that there is so much confusion around the work of the Intelligence Services Commissioner and the Interception of Communications Commissioner… We have serious doubts that either the Interception of Communications Commissioner role or the Intelligence Services Commissioner role should be part-time. We are also concerned that the extent of the Intelligence Services Commissioner's staff is one personal assistant. The fact that less than 10% of warrants which allow intrusion in to the private lives of individuals are examined is concerning… All parts of the oversight system need to do more to improve public confidence in their work… The current system of oversight belongs to a pre-internet age, a time when a person's word was accepted without question. What is needed is a scrutiny system for the 21st century, to ensure that sophisticated security and intelligence agencies can get on with the job with the full confidence of the public… Given the criticism which the Regulation of the Investigatory Powers Act is subject to, we believe that the legislation is in need of review."

Main public authorities discussed: Police, intelligence agencies, National Crime Agency

Locations referred to: worldwide

[25] United Kingdom, Parliament (2014) Home Affairs Committee - Seventeenth Report Counter-terrorism, 30 April 2014, available at: www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm.

Intelligence and Security Committee of Parliament, Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, 17 July 2013[26]

Main findings:

- "It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded.
- We have reviewed the reports that GCHQ produced on the basis of intelligence sought from the US, and we are satisfied that they conformed with GCHQ's statutory duties. The legal authority for this is contained in the Intelligence Services Act 1994.
- Further, in each case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in the Regulation of Investigatory Powers Act 2000."

Main public authorities discussed: GCHQ

Locations referred to: UK, USA

Report by the Draft Communications Data Bill Joint Committee, ordered by the House of Lords and the House of Commons to be printed 28 November 2012[27]

Main findings: "We accept that there is a case for legislation which will provide the law enforcement agencies with some further access to communications data, but we believe that the draft Bill pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data… We believe that the current safeguards on the authorisation of applications for access to data are working better than is often thought, but we make recommendations for improving them, and for strengthening the roles of the Interception of Communications Commissioner and the Information Commissioner."

Main public authorities discussed: Police, intelligence agencies, National Crime Agency, HM Revenue and Customs

Locations: communications sent or received outside the British Islands; foreign Communications Service Providers; Mutual Legal Assistance Treaties

[26]United Kingdom, Intelligence and Security Committee (2013) Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, available at: http://isc.independent.gov.uk/files/20130717_ISC_statement_GCHQ.pdf

[27] United Kingdom, Parliament (2012) Draft Communications Data Bill Joint Committee - First Report Draft Communications Data Bill, 28November 2012, available at: www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7902.htm.

Speech by the Deputy Prime Minister on Security and privacy in the internet age, Royal United Services Institute, 4 March 2014[28]

Main findings: "In an increasingly interconnected world, where the threats to our safety are also globalised, we rely more and more on intelligence-led security interventions to protect our people from harm… This is not a binary debate between good and evil… It is this set of questions:

- are the capabilities of the state proportionate to the risks we face?
- do we have the right legal frameworks to protect our citizens' human rights, freedom of communication and privacy, even as technology develops?
- do we have the right oversight regime so that the agencies and those who work in them are held to account for their activities within those frameworks?
- are we completely unstinting in the pursuit of transparency so that we are always confident that secrecy – where it is used – is a necessity, rather than simply a habit?"

Main public authority discussed: GCHQ

National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

2013 Annual Report of the Interception of Communications Commissioner, Ordered by the House of Commons to be printed on 8th April 2014[29]

Main findings: "The Regulation of Investigatory Powers Act 2000 (RIPA 2000) is a difficult statute to understand… indiscriminate retention for long periods of unselected intercepted material (content) does not occur… Lawfully intercepted related communications data are in some instances retained for a variety of longer periods. On this point, I have yet to satisfy myself fully that some of the retention periods are justified… the total number of interception errors reported to our office during the calendar year was 57… In 2013, 514,608 authorisations and notices for communications data under RIPA 2000 Part I Chapter II were

[28] United Kingdom Government (2014) Security and privacy in the internet age, 4 March 2014, available at www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age
[29] United Kingdom, Interceptions Communications Commissioner (2013) 2013 Annual Report of the Interception of Communications Commissioner, available at: http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

approved [from] 214 public authorities… 87.7% of the 514,608 authorisations and notices were made by police forces and law enforcement agencies, 11.5% by the intelligence agencies and less than 1% by local authorities and other public authorities… There are also certain respects in which the accommodation and technical facilities available to me are not yet sufficient or appropriate… despite being entirely independent, we are accommodated on the Home Office estate, a department we inspect… On 9th December 2004, the Investigatory Powers Tribunal (IPT), in Open Rulings on Preliminary Issues of Law, considered the lawful integrity of section 8(4) of RIPA 2000… it is, I think, pertinent to ask what has changed since 2000 or 2004 so that a statutory procedure which was re-enacted in 2000, and whose integrity was judged to be intact in 2004, may now have become inadequate and outdated."

Following the Snowden media disclosure, the Interception of Communications Commissioner also examined the allegations concerning GCHQ's operational activities including the misuse of its powers and engagement in mass surveillance, as it was considered by the Commissioner that the questions raised by the media disclosure concerning the interception of communications fell within the scope of his statutory oversight responsibility. To this end the Commissioner investigated the media disclosures with two objectives in mind:

"• to investigate and be able to report on the lawfulness (or otherwise) of relevant interception activities which UK interception agencies may undertake or have undertaken.
• to address and report on a variety of concerns which have been expressed publicly in Parliament or in the media arising out of the media disclosures."

The Commissioner summarised his findings in the following key points:

"I have considered in detail the large question whether RIPA 2000 Part I remains fit for its required purpose in the developing internet age. I have concluded that it is as fit for purpose as it was when it was enacted. I need to carry out further investigations into one aspect of the operation of Section 8(4)……Public authorities do not misuse their powers under RIPA Part I to engage in random mass intrusion into the private affairs of law abiding UK citizens. It would be comprehensively unlawful if they did. I have considered whether there is a material risk that unlawful intrusion might occur in the operation of Section 8(4). Subject to some further investigation, I conclude there is no material risk. ……I am quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant……British intelligence agencies do not circumvent domestic oversight regimes by receiving from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK."

Main public authorities discussed: Police, intelligence agencies, National Crime Agency, HM Revenue and Customs

Locations referred to: UK, USA

Report of the Intelligence Services Commissioner for 2013

Main findings: "There has been debate about whether RIPA, an Act published in 2000, can still apply when technology has advanced significantly since that time. Of the many techniques used which take advantage of technological capabilities now available, some could not have been envisioned when RIPA was drafted. But the Act was written to take account of technological change so as such the wording of the Act is technology neutral. RIPA was also written to reflect Human Rights legislation, which remains current, so it still applies. I am satisfied that the agencies apply the same authorisation process and the same test of necessity and proportionality with these more advanced technologies as they do with simpler, more traditional ones… When I first took up my role I was concerned that twice yearly inspections and a sample of warrants might not be sufficient. However, taking into account the method of my review as set out in Chapter 2, the robust and rigorous internal compliance tests and assurances, and the culture and ethos of the intelligence services, I am satisfied that it is sufficient…

Throughout 2013 there were allegations in the media that GCHQ had been conducting activities unlawfully. The first allegation suggested that GCHQ had circumvented UK law. When I read about it, I was extremely concerned, as many other people were. However, as the Intelligence Services Commissioner, I was able to visit GCHQ immediately and confront them about the allegations. I first did so on 13 June 2013, and again on 10 July during a pre-arranged visit.

During these two visits, I was first briefed in depth about the agency's activities and the allegations. I then met and questioned a number of senior GCHQ officials, including a GCHQ lawyer. My questions were probing and challenging. I also questioned Sir Iain Lobban, the Director of GCHQ. The results of this questioning and briefing allowed me to conclude that GCHQ were not circumventing the law in the UK. Everyone I spoke to was forthcoming and answered all my questions fully and willingly…

I made it clear to the agencies that any inappropriate use of, or access to, operational data is unacceptable. This is an area covered during my oversight visits and I am satisfied that the agencies have robust systems in place to detect wrongdoing and strict procedures for disciplining staff if wrongdoing has occurred."

Main public authorities discussed: Intelligence agencies, Ministry of Defence, Home Office, Foreign Office, Northern Ireland Office

Locations referred to: UK, (unspecified) other countries

Report of the Intelligence Services Commissioner for 2012, Ordered by the House of Commons to be printed on 18 July 2013[30]

[30] United Kingdom, Intelligence Services Commissioner (2012) Report of the Intelligence Services Commissioner for 2012, available at: http://isc.intelligencecommissioners.com/docs/Intelligence%20Services%20Commissioner%202013%20V8%20WEB.pdf

Main findings: "Based on my scrutiny of GCHQ warrants and authorisations, it is my belief that the activity that GCHQ undertakes is carried out under appropriate authorisation and is necessary for GCHQ's statutory purposes. In addition, I have sought, and received, assurances that considerations of the proportionality of any operations includes an assessment of whether the expected intelligence gained justifies the level of intrusion into privacy. During my December visit I agreed with GCHQ how this privacy element of proportionality could be more clearly set out in the formal submissions for warrants and authorisations.
I reiterate my comment made last year that it is my belief, based on what I have seen during my scrutiny inspections and under-the -bonnet visits, that GCHG [sic] staff conduct themselves with the highest level of integrity and legal compliance."

Main public authorities discussed: Intelligence agencies, Ministry of Defence

Locations referred to: UK, overseas

Non-governmental organisations (NGOs), Academic and research institutes, think tanks, investigative media report.

Open Rights Group, Digital surveillance - Why the Snoopers' Charter is the wrong approach: A call for targeted and accountable investigatory powers, 29 April 2013[31]

Main findings: "There is vastly more information now about our every movement than there ever has been… Much of it, for example information from social media or our web histories, can be incredibly intrusive… Just because information is useful to law enforcement does not mean that the state, or law enforcement agencies, or public bodies should be able to order its collection or have access to it… The Government's current proposals, in the form of the Communications Data Bill, is a manifestation of the temptation to grab data where it exists, and of a failure to consider alternatives to blanket collection and retention of data… In providing context and recommendations, the articles in this report offer a basis for a conversation about proportionate surveillance laws in the digital age."

Main public authorities discussed: Police, intelligence agencies, National Crime Agency, HM Revenue and Customs

Locations referred to: UK, overseas

[31]United Kingdom, Open Rights Group (2013) Digital Surveillance: Why the Snoopers' Charter is the wrong approach: A call for targeted and accountable investigatory powers, 29 April 2013, available at www.openrightsgroup.org/ourwork/reports/digital-surveillance/.

David Omand, Jamie Bartlett and Carl Miller, #Intelligence, London: Demos, 2012[32]

Main findings: "social media intelligence – which we term 'SOCMINT' – could contribute decisively to public safety: identifying criminal activity; giving early warning of disorder and threats to the public; or building situational awareness in rapidly changing situations… Democratic legitimacy demands that where new methods of intelligence gathering and use are to be introduced they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved, even if the operational details of the sources and methods used must sometimes remain secret… what is 'public' and what is 'private' is not always obvious, and differs greatly across social media platforms and even within social media platforms… Ensuring intelligence and security work is proportionate, legitimate and based on public consent depends on measuring and managing the possible harms it might entail; for SOCMINT how this is to be done is still unclear… SOCMINT must be based on a publicly argued and sound legal footing, with clarity and transparency over use, storage, purpose, regulation and accountability… SOCMINT must be able to produce reliable, powerful insight that can be acted on. This means there needs to be greater investment in human and technology capabilities."

Main public authorities discussed: Police, intelligence agencies, National Crime Agency

Locations referred to: UK, overseas

Big Brother Watch, Enhancing surveillance transparency: A UK policy framework, 2014[33]

Main findings: "The public should be able to know who has used what powers, how often, and why. They should also be informed about the effectiveness of surveillance and whether data is being collected in bulk… Already far more detailed data is available in the US about how surveillance powers are used and there has not been a discernible reduction in law enforcement effectiveness… 70% of British adults say British companies should publish reports on how often they receive requests for customer data from the police and security services. 66% of British adults say that the Government should publish more data about how surveillance powers are used."

Main public authorities discussed: Police and intelligence agencies

Locations referred to: UK, USA

[32] United Kingdom, Demos (2012) #Intelligence, available at www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327
[33] United Kingdom, Big Brother Watch (2014) Enhancing surveillance transparency: A UK policy framework, 2014, available at www.bigbrotherwatch.org.uk/files/briefings/BBW_transparency_2014.pdf

Guardian News, GCHQ, 2014[34]

The Guardian has an extensive archive of articles relating to the Edward Snowden disclosures.

The Register, 2014[35]

The Register has reported a number of details of the disclosures witheld by other media, such as details of Middle East surveillance in the article Revealed: GCHQ's Beyond Top Secret, Middle Eastern Internet Spy Base, by Duncan Campbell, 3 June 2014.

[34] United Kingdom, Guardian News (2014) GCHQ, available at www.theguardian.com/uk/gchq/
[35] United Kingdom, The Register (2014) Revealed: GCHQ's Beyond Top Secret, Middle Eastern Internet Spy Base, available at www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base/