Interception of communications

Standard Note: SN/HA/6332

Last updated: 13 March 2015

Author: Philip Ward and Alexander Horne

Section Home Affairs

Interception of communications takes two forms: the collection and monitoring of *communications data* (e.g. records of who contacted whom, when, from where and for how long) and interception of the *content* of the communications themselves. Interception was not put on a statutory footing until the *Interception of Communications Act 1985*. Rapid changes in telecommunications prompted a Government consultation in 1999, which resulted in the passage of the present law, the *Regulation of Investigatory Powers Act 2000* (RIPA).

Under RIPA, authorisations for the acquisition and disclosure of communications data are issued by "designated persons" within the organisation seeking the data. In order to gain access to the *actual content* of a communication (for example the text of an email message or a telephone conversation) then a warrant issued by the Secretary of State is generally required.

Under a 2006 EC Directive incorporated into UK law since 2009, communications service providers (telephone companies and internet service providers) were required to retain communications data for a year. In April 2014, the European Court of Justice declared the 2006 Directive invalid. In response to the resulting uncertainty, the Government introduced the *Data Retention and Investigatory Powers Act 2014* (DRIP), a fast-tracked piece of legislation passed with cross-party agreement by both Houses in July 2014.

A *draft Communications Data Bill* was announced in the Queen's Speech in 2012 and published on 14 June 2012. The Bill was subject to pre-legislative scrutiny and some aspects of the Government's proposals were criticised. Frequently referred to by critics as a "snooper's charter", it was opposed by the Liberal Democrats and not taken forward in the 2012-13 session. The draft Bill would have extended powers to cover messages sent on social media, webmail, voice calls over the internet and gaming in addition to emails and phone calls.

This Note looks at past and present law, the role of the Interception of Communications Commissioner in overseeing the present regime and recent developments in this area.

Contents

1 Introduction

"Interception of communications" is a generic term used to refer to the monitoring and scrutiny of private messages between individuals or organisations, it is important to make a distinction – as the law does – between "communications data" and "content". "Communications data" usually refers to information about a message that has been sent via a network or service, as opposed to the actual *contents* of that message.

2 RIPA

The *Regulation of Investigatory Powers Act 2000* (RIPA) provides a framework for lawful interception of communications, access to communications data, surveillance and the use of covert human intelligence sources (undercover agents).[1] Part I, Chapter I deals with interception. Part I Chapter II covers with the acquisition and disclosure of communications data.

RIPA's associated codes of practice lay stress on the need for exercising investigatory powers in ways that are both necessary and proportionate. RIPA itself sets out the possible justifications for interference with an individual's right to privacy as embodied by the *Human Rights Act 1998*:

- In the interests 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.
- For the purpose (in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant for the purpose of preventing or detecting serious crime) of giving effect to the provisions of any international mutual assistance agreement.[2]

2.1 Interception of communications

Part 1 Chapter 1 of RIPA provides the relevant legal framework to intercept the *content* of communications (by post as well as telephone and email).

Section 1 makes it an offence, subject to exceptions, to intercept a public or private telecommunication (this will apply to mobile phones as well as landlines[3]):

> The statutory framework comprises two general offences of unlawful interception, followed by exceptions in which interception will be lawful.
>
> The two general offences are intercepting a public postal or telecommunication without lawful authority (s 1(1) RIPA, a crime) and unauthorized interception on a private telephone system (s 1(2) and (3) RIPA, a tort).[4]

Lawful interception can take place in a number of ways:

- Where a warrant has been issued by the Secretary of State under section 5

---

1 In Scotland, surveillance and covert human intelligence sources fall within the *Regulation of Investigatory Powers (Scotland) Act 2000*

2 s5(3)(a)-(d)

3 Section 2 of the Act provides the relevant definition of "public telecommunication system"

4 Clive Harfield and Karen Harfield, *Covert Investigation* (Oxford, 2005)

- Sections 3 and 4 provide for some circumstances where interception without a warrant is lawful.

In relation to section 3, the Act's explanatory notes[5] summarises the situation thus:

> This Section authorises certain kinds of interception without the need for a warrant under Section 5, namely where one or more parties to a communication have consented to the interception, conduct is in relation to the provision or operation of services, or conduct takes place with the authority of a person designated for the purposes of the Wireless Telegraphy Act 1949.

And for section 4:

> This Section lists the cases where a power may be exercised to provide for lawful interception without the need for a warrant under Section 5: under an international mutual assistance agreement; under regulations made by the Secretary of State to permit certain kinds of interception in the course of lawful business practice; under prison rules; in hospital premises where high security psychiatric services are provided; and in state hospitals in Scotland.

Before giving a warrant, the Secretary of State must be satisfied that interception is necessary to obtain the information required; that the information could not reasonably be obtained by other means; and the interception is *proportionate* to what it seeks to achieve.[6]

The Act makes provision (section 7(l)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. The Act restricts issue of warrants in this way to urgent cases where the Secretary of State has himself expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)). A warrant issued under the urgency procedure lasts for five working days following the day of issue unless renewed by the Secretary of State, in which case it expires after 3 months in the case of serious crime or 6 months in the case of national security or economic well-being in the same way as other non-urgent section 8(l) warrants. An urgent case is one in which interception authorisation is required within a twenty four hour period.[7]

There has been some confusion over what constitutes interception. Of likely relevance is the phrase "in the course of its transmission" which appears in different places in section 1 of RIPA; for example in subsection 1:

> (1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of—
>
> (a) a public postal service; or
>
> (b) a public telecommunication system.

---

5 http://www.legislation.gov.uk/ukpga/2000/23/notes/contents

6 s5(2)(b)

7 https://www.gov.uk/government/publications/code-of-practice-for-the-interception-of-communications

Section 2 of the Act explains how "in the course of its transmission" should be interpreted. Reproduced below are relevant subsections that can be read[8] as capturing both voicemails and emails:

> (2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication **in the course of its transmission** by means of a telecommunication system if, and only if, he—
>
> (a) so modifies or interferes with the system, or its operation,
>
> (b) so monitors transmissions made by means of the 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 of the communication available, **while being transmitted**, to a person other than the sender or intended recipient of the communication.
>
> [...]
>
> (7) For the purposes of this section **the times while a communication is being transmitted** by means of a telecommunication system shall be taken to **include any time when the system** by means of which the communication is being, or has been, transmitted **is used for storing it** in a manner that enables the intended recipient to collect it or otherwise to have access to it.
>
> (8) For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.
>
> [emphasis added]

Subject to a limited number of exceptions, evidence from intercepted communications or any related communications data is inadmissible in legal proceedings under provisions currently set out in section 17 of RIPA.[9]

2.2 Access to communications data

Part I, Chapter II of RIPA covers the acquisition and disclosure of *communications data*. Only persons designated under the Act, or by regulations made under it, may authorise access to communications data. And they can only do so for certain purposes (which vary according to the relevant public authority in question). Relevant forms connected with the authorisation process are available online.[10]

The relevant public authorities are specified in section 25 of the 2000 Act, as amended:

> (a) a police force;
>
> (b) the Serious Organised Crime Agency;

---

8 Victoria Williams, *Surveillance and Intelligence Law Handbook*, Oxford 2006 pp70-1

9 See the Library note on *The use of intercept evidence in terrorism trials* (SN 5249)

10 https://www.gov.uk/government/collections/ripa-forms--2

(ba) the Scottish Crime and Drug Enforcement Agency;

(d) Her Majesty's Revenue and Customs;

(f) any of the intelligence services;

(g) any such public authority not falling within paragraphs (a) to (f) as may be specified for the purposes of this subsection by an order made by the Secretary of State.

Orders have subsequently been made by the Secretary of State which have added substantially to the number of public authorities that may access communications data, for specified purposes.[11] A report (for 2006) of the Interception of Communications Commissioner, published in January 2008 states:

> Currently, the number of public authorities that I am required to inspect and oversee under Part I Chapter II of RIPA are as follows:
>
> a. The security and intelligence and law enforcement Agencies – the Security Service, Secret Intelligence Service and Government Communications Headquarters.
>
> b. The Serious Organised Crime Agency and HM Revenue and Customs.
>
> c. 52 police forces.
>
> d. 12 other Law Enforcement Agencies such as the Royal Military Police and the British Transport Police.
>
> e. 474 local authorities authorised to acquire communications data.
>
> f. 110 other public authorities such as the Financial Services Authority, the Serious Fraud Office, the Independent Police Complaints Commission, the Ambulance Service and Fire Authorities who are authorised to acquire communications data.[12]

Access to communications data requires authorisation of a senior official; in the police this means the rank of superintendent or above (an inspector can authorise access to a limited range of data – excluding traffic data for example). The relevant ranks are specified in the *Regulation of Investigatory Powers (Communications Data) Order* SI 2010/480.

In order to gain access to the *actual content* of a communication (for example the text of an email message or a telephone conversation) then a warrant issued by the Secretary of State is generally required. This would come under Part I, Chapter 1 (interception) of the 2000 Act. The security services, the police and other law enforcement agencies have access to the warrant system for interception.

RIPA authorisation is not needed in all cases. Of relevance here is *Decision No. IPT/03/32/H* (14 November 2006) in the Investigatory Powers Tribunal from which the following is extracted:

> Although RIPA provides a framework for obtaining internal authorisations of directed surveillance (and other forms of surveillance), there is no general prohibition in RIPA

---

[11] The most recent orders, superseding three earlier ones, is the *Regulation of Investigatory Powers (Communications Data) Order 2010* SI 2010/480. See also the draft *Regulation of Investigatory Powers (Communications Data) (Amendment) Order 2015.*

[12] https://www.gov.uk/government/publications/report-of-the-interception-of-communications-commissioner-2006 (HC 252)

> against conducting directed surveillance without RIPA authorisation. RIPA does not *require* prior authorisation to be obtained by a public authority in order to carry out surveillance. Lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful.[13]

The *Protection of Freedoms Act 2012* contains a wide range of measures, some of which relate to RIPA. Part 2 Chapter 2 of the Act provides for judicial approval of those types of surveillance which are available to local authorities under RIPA. The relevant surveillance activities are access to communications data and the use of directed surveillance and covert human intelligence sources (undercover agents). Library research paper 11/20 contains further details (see pages 18-22).

3 Retention of communications data

Related to the question of access to the data mentioned above, there is also the question of its retention in the first place. RIPA as originally enacted applied only to communications data collected after the authorisation had been issued. Law enforcement agencies argued that, to facilitate successful prosecutions, they needed access to historical data as evidence, since by the time a plot was uncovered, it might already be well advanced.

A voluntary Code of Practice on the Retention of Communications Data had existed since 2003. Under the *Anti-Terrorism, Crime and Security Act 2001* (ATCSA) telecommunications operators were asked to retain information on a voluntary basis with the understanding that they would be reimbursed for retaining and handing over data beyond their normal operations. A code of practice setting out the voluntary agreement was created through the *Retention of Communications Data (Code of Practice) Order 2003*.

Directive 2006/24/EC on retaining data generated through electronic communications or public communications networks was originally implemented in the UK by the *Data Retention (EC Directive) Regulations* SI 2007/2199. These came into force on 1 October 2007 since when the retention (for a year) of specified data became mandatory while the reimbursement of costs remained as under the voluntary system.

The *Data Retention (EC Directive) Regulations* SI 2009/859 came into force on 6 April 2009. These regulations superseded and revoked the *Data Retention (EC Directive) Regulations* SI 2007/2199 extending the latter to include internet activity among the communications data that must be retained (for a year) by public communications providers. As a result of these later regulations, the UK completed its transposition of Directive 2006/24/EC. A schedule to the 2009 regulations detailed the communications data that were to be retained (any unconnected calls were not covered). For example, in the context of fixed network telephony, the following was among the data to be retained under the regulations:

> Data necessary to trace and identify the source of a communication
>
> 1.—(1) The calling telephone number.
>
> (2) The name and address of the subscriber or registered user of any such telephone.
>
> Data necessary to identify the destination of a communication
>
> 2.—(1) The telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred.

---

[13] Investigatory Powers Tribunal Decision No: IPT/03/32/H, 14 November 2006

(2) The name and address of the subscriber or registered user of any such telephone.

An important caveat to the above was regulation 10 of the 2009 regulations:

> **10.**—(1) These Regulations do not apply to a public communications provider unless the provider is given a notice in writing by the Secretary of State in accordance with this regulation.

The Home Office confirmed in September 2009 that it had issued Notices to "several" Communication Service Providers (CSPs) since the Regulations came into effect on 6 April 2009. However, these have not been identified.

3.1 The 'DRIP' Act

In April 2014, the European Court of Justice declared the 2006 Directive invalid. As stated above, this Directive had been transposed into UK law by way of secondary legislation (the 2009 Regulations) and enables communication service providers to retain communications data for law enforcement purposes for periods of between six months and two years. In response to the resulting uncertainty, the Government introduced the *Data Retention and Investigatory Powers Act 2014* (DRIP), a fast-tracked piece of legislation passed by both Houses in July 2014. The Government argued that emergency legislation was needed to ensure that UK law enforcement and intelligence agencies could maintain their ability to access the telecommunications data they needed to investigate criminal activity and protect the public. There was cross-party agreement on the need for the legislation. It has a sunset section, so that the provisions expire at the end of 2016. The 2014 Act provides powers to replace the 2009 Regulations.[14] Further detail is available in Library Standard Note 6934, *The Data Retention and Investigatory Powers Bill.*

3.2 The draft *Communications Data Bill*

The *draft Communications Data Bill* was announced in the Queen's Speech in 2012 and it was published on 14 June 2012. The Bill was subject to pre-legislative scrutiny and some aspects of the Government's proposals were criticised. The Bill was frequently referred to by critics as a "snooper's charter" and it was not taken forward in the 2012-13 session. New Government proposals on cybercrime were foreshadowed in the 2013 Queen's Speech, but these appear to be more limited than the plans set out in the draft Bill.

The *draft Communications Data Bill* was scrutinised by a Joint Committee of both Houses of Parliament (the Joint Committee), and was also considered by the Joint Committee on Human Rights (JCHR) and the Intelligence and Security Committee (ISC).

The Government indicated the purpose of the draft Bill was "to protect the public and bring offenders to justice by ensuring that communications data is available to the police and security and intelligence agencies." The draft Bill would have extended powers to cover messages sent on social media, webmail, voice calls over the internet and gaming in addition to emails and phone calls. The data could have included the time, duration, originator and recipient of a communication and the location of the device from which it is made. However, it is important to note that it would not have included the content of messages (i.e. what was being said or communicated). The draft Bill also contained provisions that would have restricted the type of information available to local authorities and other public bodies.

---

[14] The *Data Retention Regulations 2014* (SI 2014/2042) were made under the 2014 Act.

Reaction to the draft Bill was mixed, with privacy groups and other NGOs expressing concerns. The Joint Committee published its report on 11 December 2012. It concluded that the scope of the Bill should be significantly narrowed, whilst recognising that more needed to be done to provide law enforcement and other agencies with access to data they cannot currently obtain. The Intelligence and Security Committee published a separate report (relating to the intelligence services) on 5 February 2013.

Initially, it was suggested that the Bill would be redrafted to meet concerns that had been raised; however in April 2013 it was reported that the Deputy Prime Minister had said in a radio interview that "what people have dubbed the snooper's charter" was "not going to happen". [15] He reiterated his position in a radio interview in January 2015 in the wake of the shootings in Paris at the offices of the satirical magazine *Charlie Hebdo*.[16]

Further information may be found in a Library Standard Note, *Communications data: the draft Bill and recent developments* (SN 6373).

Another Library Note, *Internet surveillance* (SN 6304), looks at the history of two programmes which formed a backdrop to the draft Bill: the Communications Capabilities Development Programme and an initiative under the previous Government, the Interception Modernisation Programme. That Note also cites the justifications given by successive governments for what critics have dubbed a "snooper's charter" and details some of the objections that have been raised against surveillance of this sort.

4 Scrutiny

Oversight of access to communications data (and interception of its content) is carried out by the Interception of Communications Commissioner. The Office of Surveillance Commissioners is responsible for oversight of property interference under Part III of the *Police Act 1997*, as well as surveillance and the use of covert human intelligence sources by all organisations bound by RIPA (except the Intelligence Services). The Investigatory Powers Tribunal investigates complaints about the use of RIPA powers.

The aspects of RIPA that deal with communications intercepts and access to communications data are overseen by the Interception of Communications Commissioner, The Right Honourable Sir Anthony May. He keeps under review:

- the Secretary of State's role in issuing warrants for the interception of communications
- the procedures adopted by those agencies involved in interception under warrant, to ensure they are compliant with RIPA.
- the procedures adopted by any other organisations that assist those agencies in warranted interception.
- the adequacy of arrangements made by the Secretary of State for the handling and protection of intercepted material.

With the commencement of Part I Chapter II, and Part III of RIPA, the Interception of Communications Commissioner also has responsibility for overseeing:

---

15 *BBC Online*, "Nick Clegg: No 'web snooping' bill while Lib Dems in government", 25 April 2013

16 "Nick Clegg: Snooper's charter would not plug intelligence gap", *Guardian*, 13 January 2015

- the work of all organisations involved in the acquisition of communications data.
- notices authorised by the Secretary of State ordering the decryption of data acquired by interception.
- the adequacy of arrangements made by the Secretary of State for the protection of communications data and encryption keys for intercepted material.

Part of the Commissioner's oversight regime includes biannual inspection visits to those agencies conducting warranted interception and the departments of the relevant Secretaries of State. He also makes annual visits to communications service providers charged with maintaining an interception capability and providing assistance to the agencies.

All members of an organisation that has carried out or given assistance in the interception of communications, are required to provide any information and assistance to enable the Commissioner to carry out his functions.

On 5 January 2004, Chapter II of Part I of RIPA came into force enabling specific organisations approved by Parliament to acquire communications data. In view of the number of organisations empowered, a Chief Inspector and a team of Inspectors were appointed to support the Commissioner in his oversight responsibility for this area of his work.

All oversight under Chapter I of Part I of RIPA (Interception of Communications) continues to be carried out by the Commissioner himself.

All breaches of legislation or Codes of Practice are reported to the Commissioner and included in his annual report to the Prime Minister, which also documents his findings on the work of the Security, Intelligence and law enforcement agencies throughout the previous year. The Prime Minister then lays a copy of the report before each House of Parliament.

Under Sir Anthony May's predecessor, the report was divided into a publishable section and a confidential annexe. The publishable section included as much information as possible without compromising the work of the intelligence services and law enforcement agencies. The confidential annexe was not published due to its sensitivity. In his latest report (for 2013) the current Commissioner indicated that he was taking a different approach:

> **1.7** It is not so easy to give a relevant public account of what the interception agencies actually do because much of it is sensitive. In this report, I am constrained by statutory provisions forbidding disclosure. But an important change of presentation in this report is that I shall try to be more informative than my predecessors felt they needed to be. To this end, I am not submitting any suggested Confidential Annex to this report to the Prime Minister. I do not consider that a confidential annex is presently necessary. That does not mean that one may not be needed in the future.[17]

It is strictly for the Prime Minister to decide which parts of this report should be made public by laying them before Parliament.[18] The report includes statistics on interception warrants under RIPA and a list of public authorities with access to communications data.

---

[17] 2013 Annual Report of the Interception of Communications Commissioner, 8 April 2014, HC 1184 2013-14

[18] *Regulation of Investigatory Powers Act 2000* s58(7)

5 Recent developments

5.1 Intelligence and Security Committee

The Intelligence and Security Committee of Parliament (ISC) announced on 17 October 2013 that it would be broadening its inquiry into the laws which govern the intelligence agencies' ability to intercept private communications.[19] It held public evidence sessions in October 2014 as part of its Privacy and Security Inquiry. These sessions explored a number of themes, including:

> expectations of privacy, and the extent to which it may be appropriate to intrude into an individual's privacy in order to protect the rights and safety of others;
>
> whether it is acceptable to use intrusive capabilities in a targeted way against known threats, and whether it is ever acceptable to use such capabilities to gather information in larger quantities;
>
> whether the current statutory framework governing and regulating the Agencies' intrusive activities delivers those principles; and,
>
> whether there is scope for greater transparency in this area.[20]

The Committee published its report on 12 March 2015. Although they were satisfied that the UK's intelligence and security agencies do not seek to circumvent the law when carrying out surveillance, the ISC had misgivings about those existing laws. The legal framework had developed "piecemeal" and was "unnecessarily complicated", the Committee felt, resulting in a lack of transparency which was not in the public interest:

> Our key recommendation therefore is that the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This must clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so.[21]

5.2 The Anderson Review

The Home Secretary, Theresa May, announced on 10 July 2014 that she had asked David Anderson QC, the Independent Reviewer of Terrorism Legislation, to lead a review, before the general election, of the capabilities and powers required by law enforcement and intelligence agencies, and the regulatory framework within which those capabilities and powers should be exercised.[22] The *Data Retention and Investigatory Powers Act 2014* (s7) requires the Secretary of State to initiate this review: its terms of reference are available online. Mr Anderson will assess whether Part 1 of RIPA should be amended or replaced and examine the effectiveness of current arrangements for statutory oversight. He has said:

> Among the issues I have been asked to look at are whether the UK needs new legislation along the lines of the proposed Communications Data Bill, and whether Part 1 of RIPA 2000 (which deals both with interception and with communications data) needs to be amended or replaced. I will also be looking at the statistical and transparency requirements that should apply, and at the effectiveness of current statutory oversight arrangements. For comparative purposes I expect to refer to the

---

19 Intelligence and Security Committee press release, 17 October 2013
20 Intelligence and Security Committee press release, 9 October 2014
21 Intelligence and Security Committee, *Privacy and security: a modern and transparent legal framework*, HC 1075 2014/15, 12 March 2015, p2
22 HC Deb 10 July 2014 c463

> position in other countries, in particular Germany and the USA which I propose to visit.[23]

5.3 Independent Surveillance Review

On 4 March 2014, the Deputy Prime Minister, Nick Clegg, announced an independent Surveillance Review (ISR), to be carried out by the Royal United Services Institute (RUSI). This review into surveillance technologies and the problems of control and oversight will examine surveillance practices in the UK in the context of new communications technologies. It will make recommendations for legislative and policy reform and will deliver a report after the next general election to be considered by the Government alongside the Intelligence and Security Committee review and the Anderson review.[24]

5.4 IOCC inquiry

On 6 October 2014, the (acting) Interception of Communications Commissioner, Sir Paul Kennedy, launched an inquiry to determine whether the acquisition of communications data had been used to identify journalistic sources.[25] He wrote to all Chief Constables and directed them, under section 58(1) of RIPA, to provide him with details of all investigations that had used powers under Chapter 2 of Part I of RIPA to acquire communications data to identify journalistic sources. He said that his office would undertake a full inquiry into these matters and report the findings to the Prime Minister and publish them.[26]

On 4 February 2015, Sir Anthony May published his report into the use by police of RIPA to access journalists' communication records. His inquiry found that some 82 journalists had had their communications data obtained by police in three years. Sir Anthony concluded that police forces "did not give due consideration to freedom of speech" and current and Home Office guidelines did not sufficiently protect journalistic sources. He also recommended that police forces should be required to seek a judge's permission when seeking to discover a journalist's confidential source.[27]

5.5 Home Affairs Committee

On 6 December 2014 the Home Affairs Committee published the report of its inquiry into police forces' use of RIPA powers to acquire communications data in the course of investigations.[28] The Committee argued that current systems of oversight are inadequate and that any updated RIPA Code of Practice should contain special provisions for dealing with privileged information, such as journalistic material and material subject to legal privilege:

> 33. RIPA is not fit for purpose, with law enforcement agencies failing to routinely record the professions of individuals who have had their communications data accessed under the RIPA. The recording of information under RIPA is totally insufficient, and the whole process appears secretive and disorganised with information being destroyed afterwards. Whereas we acknowledge the operational need for secrecy both during

---

23 Investigatory Powers Review: call for evidence, 21 July 2014

24 RUSI News, *RUSI to convene independent review on the use of internet data for surveillance purposes*, 4 March 2014. This press notice includes the review's terms of reference.

25 Sir Anthony May was involved in a road traffic accident in the summer of 2014 and suffered serious injuries. Sir Paul Kennedy was appointed as interim Commissioner by the Prime Minister to cover in Sir Anthony's absence. Sir Anthony resumed his duties in January 2015. See IOCCO press notice, 1 January 2015

26 IOCCO press notice, *IOCCO launches inquiry into the use of RIPA powers to acquire communications data relating to the confidential sources of journalists*, 6 October 2014

27 Interception of Communication Commissioner's Office, *IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources*, 4 February 2015

28 Home Affairs Committee, *Regulation of Investigatory Powers Act 2000*, 6 December 2014, HC711

> investigations and afterwards (so that investigative techniques more broadly are not disclosed), we are concerned that the level of secrecy surrounding the use of RIPA allows investigating authorities to engage in acts which would be unacceptable in a democracy, with inadequate oversight. We recommend that the Home Office use the current review of the RIPA Code to ensure that law enforcement agencies use their RIPA powers properly.

5.6 Codes of practice

On 9 December 2014 the Government launched a consultation on two draft codes of practice on communications data. The closing date for responses was 20 January 2015. The first is an updated acquisition and disclosure of communications data code of practice pursuant to s71 of RIPA. The second is a new retention of communications data code of practice pursuant to regulation 10 of the *Data Retention Regulations 2014* and s71 of RIPA:

> The draft codes of practice set out the processes and safeguards governing the retention of communications data by communications service providers and its acquisition by public authorities, including law enforcement agencies. They are intended to provide clarity, and incorporate best practice, on the use of the relevant powers, ensuring the highest standards of professionalism and compliance in this important aspect of law enforcement.
>
> The consultation seeks views on the additional consideration that must be given to communications data requests relating to those in professions which handle confidential information (such as journalists). The consultation also contains a document setting out how the retention code of practice would take into account provisions contained in the Counter-Terrorism and Security Bill.[29]

The two draft Codes were subsequently laid before both Houses for approval:[30]

First, the draft *Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order* 2015, which is summarised as follows in the associated draft Explanatory Memorandum:

> 7.5 The main changes to the acquisition code concern the provision of additional safeguards. The code enhances the operational independence of authorising officers in relevant public authorities. Further changes include reflecting the additional requirements on local authorities to request communications data through a magistrate and the National Anti-Fraud Network; new record keeping requirements for public authorities; and aligning the code with best practice regarding providing communications data to the emergency services following an emergency call.
>
> 7.6 The Interception of Communications Commissioner has recommended that judicial approval should be applied where the police request communications data in order to identify a journalist's source. The acquisition code therefore requires the police to use a Production Order under the Police and Criminal Evidence Act 1984 ('PACE'), which requires judicial approval, rather than RIPA, to request communications data in such circumstances. It also specifies that additional consideration to the level of intrusion must be given, in terms of both privacy and, where applicable, freedom of expression, when considering whether to acquire communications data involving professionals who handle privileged or otherwise confidential material.

---

29 https://www.gov.uk/government/consultations/communications-data-codes-of-practice-acquisition-disclosure-and-retention

30 They are scheduled to be debated and approved in the Commons on 16 March 2015.

And second, the draft *Retention of Communications Data (Code of Practice) Order 2015*. The associated draft Explanatory Memorandum offers this summary:

> 7.3 DRIPA and the Regulations made under it replaced the UK's previous data retention regime, while adding a number of safeguards. One of these important changes provided for a statutory code of practice on communications data retention in order to provide clear guidance on best practice.
>
> 7.4 The new retention code sets out how the Government implements the requirements in DRIPA and the Data Retention Regulations. It covers the issue, review, variation and revocation of data retention notices; the CSPs' ability to recover their costs; data security; oversight by the Information Commissioner; and safeguards on the disclosure and use of retained data by CSPs. It also outlines the scope and definitions of relevant communications data, including data that may be retained following provisions in CTSA [the *Counter-Terrorism and Security Act 2015*].

5.7 Counter-Terrorism and Security Act 2015

Part 3 of the *Counter-Terrorism and Security Act 2015* amends the *Data Retention and Investigatory Powers Act 2014* to enable the Secretary of State to require internet service providers to retain data allowing the authorities to identify the person or device using a particular IP address at any given time.[31] The Bill's accompanying ECHR memorandum indicates the value of such data to the intelligence and law enforcement agencies:

> 25. Communications data is used by the intelligence and law enforcement agencies during investigations regarding national security, as well as serious and organised crime. It enables investigators to identify members of a criminal network, place them in specific locations at given times and in certain cases to understand the criminality in which they are engaged. Communications data can be vital in a wide range of threat to life investigations, including the investigation of missing persons. Communications data can be used as evidence in court.

The Bill's Privacy Impact Assessment provides further details, including the following:

> The new legislation will provide for the retention of communications data by communications service providers which will allow those authorities who are designated under the Regulation of Investigatory Powers Act 2000 (RIPA) and lawfully allowed to access traffic data, to identify who in the real world was using an IP address at a given point in time. The Bill will ensure that UK service providers retain sufficient internet communications data to allow law enforcement to attribute communications to people or their devices.

6 Appendix: the law prior to 2000

Prior to 1985, there was no statutory regulation of interception. Interception of all kinds was carried out under the Royal Prerogative. The only oversight was via the informal "judges' rules".[32] The first statutory regime, the *Interception of Communications Act 1985*, was introduced following a successful legal challenge by James Malone in a case before the European Court of Human Rights. The Strasbourg court found that since telephone tapping in Britain was not "prescribed by law", Article 8 of the European Convention on Human Rights had been contravened. Article 8 protects the individual against arbitrary interference by public authorities in his private or family life. That judgment led directly to the 1985 Act. The Act:

---

[31] HC Library Research Paper 14/63, *Counter-Terrorism and Security Bill*, 27 November 2014, pp33-7

[32] LSE, *Briefing on the Interception Modernisation Programme*, April 2009, p7

(a) created an offence of unlawful interception of communications by post or by means of a public telecommunication system.

(b) established a framework controlling issue, renewal, modification and cancellation of warrants authorising interception of communications sent by post or by means of a public telecommunication system.

(c) enshrined in law the principle that warrants may only be issued by the Secretary of State, and specified the purposes for which warrants may be issued as:

(i) in the interests of national security;

(ii) for the purpose of preventing or detecting serious crime; or

(iii) for the purpose of safeguarding the economic well-being of the United Kingdom.

(d) placed strict safeguards on the extent to which intercepted material may be disclosed, copied and retained, requiring arrangements to be made to ensure that each of these is kept to a minimum.

(e) established an independent oversight regime in the form of the Interception Commissioner, whose job is to keep under review the way in which the power to issue warrants is exercised and the operation of the safeguards described above.

(f) set up a Tribunal to investigate complaints where the complainant believes that their communications have been intercepted in breach of the Act.

A useful summary of interception powers as they existed at the time is contained in the Government consultation paper published in 1999, *Interception of Communications: A Consultation* (Cm 4368). The paper commented:

> 3.14 Provision of communications data by telecommunications operators is currently authorised by a variety of statutes. Both s45 *Telecommunications Act 1984* (as amended by IOCA) [*Interception of Communication Act 1985*] and s28 *Data Protection Act 1984* (soon to be replaced by the 1998 Act) allow holders of such data to provide it voluntarily for specific purposes, including the prevention or detection of crime, the purposes of criminal proceedings and in the interests of national security. In addition a holder of communications data may be required to produce it in obedience to a Production Order, which can be applied for under a variety of statutes and is authorised by a Crown Court judge.

The executive summary to the consultation paper indicated that:

> The Government believes that the law surrounding access to communications data is in need of revision. Itemised billing, for example, can be of tremendous investigative value, and it is right that in certain circumstances the authorities should be able to access this material. However, it also involves a measure of intrusion into individual privacy and it is essential that access should be carefully controlled in accordance with ECHR proportionality requirements, authorisation only being given where necessary and justified for clearly defined purposes. For these reasons we are proposing to establish a clear, statutory framework for access to communications data.

The paper set out a series of proposals in relation to communications data:

> 10.1 Because the analysis of communications data can provide much information about the way in which people live their lives, this has led to concerns that the level of

intrusion into an individual's privacy may be too great and that the ability of the law enforcement, security and intelligence agencies to access this data should be regulated.

10.2 The Government believes that there is a balance to be struck between the privacy of the individual and the needs of society as a whole to be protected from crime. It is right that the police have access to communications data when necessary in order to prevent or detect crime, but only where this level of intrusion is justified, taking into account the lower level of intrusion that access to such data brings.

10.3 In recent years, advances in telecommunications have meant that the amount of data held by communications service providers has increased, making the information much more useful as an investigative tool. But so has the potential for privacy infringements. Although accessing a person's communications data is not as intrusive as interception, it clearly still represents an interference with the privacy of the individual. The Government therefore believes it is time to put in place a statutory framework for authorising access to communications data.

10.4 The Government proposes to introduce a statutorily based framework to regulate access to communications data by investigating bodies. This will lay down the purposes for which an application for access to communications data may be made, the minimum standards of information which must be included within an application and the factors which must be taken into account by the authorising official. We also propose to introduce strict statutory requirements regarding the handling, storage and retention of communications data. It is intended that these measures will be laid out in detail in the publicly available Code of Practice (see paragraph 7.16).

10.5 The proposed purposes for which data access may be authorised are:

(a) for the prevention or detection of crime;

(b) for the apprehension or prosecution of offenders;

(c) in the interests of national security;

(d) for the purpose of safeguarding the economic well-being of the United Kingdom;

(e) for the urgent prevention of injury or damage to health; and

(f) for the assessment or collection of any tax or duty or of any imposition of a similar nature.

10.6 Where a request has been properly authorised in accordance with the arrangements outlined above, the communications service provider will be required to provide the specified material within a reasonable period.

Safeguards

10.7 The disclosure of data falls within the remit of the Data Protection Act 1984 (soon to be replaced by the Data Protection Act 1998), therefore the oversight and complaints mechanisms will continue to be provided under this legislation.

The Government welcomes comments on the proposals outlined in this Chapter, particularly from Communication Service Providers and bodies which make use of communications data."

Following the consultation, the Government legislated on the issue of communications data under Chapter II of the *Regulation of Investigatory Powers Act 2000*.

The 1985 Act only applied to communications sent by post or "public telecommunications systems", however, and not to such private systems as the internal phone network of an office. This led the Strasbourg Court to again find the UK in breach of Article 8 in its 1997 ruling in *Halford*. This, in turn, led the Government to publish the abovementioned 1999 White Paper which proposed fresh legislation to deal with both interception of communications and communications data. This was overtaken, however, by proposals to establish a broader statutory framework governing surveillance powers as a whole: the *Regulation of Investigatory Powers Act 2000.*

The NGO, JUSTICE, provided a detailed critique of legal provisions relating to communications data in its 2011 paper *Freedom from Suspicion: Surveillance Reform for a Digital Age* (at chapter 4). It suggests that prior to the 2000 Act, other public bodies sought data under "various specific provisions, e.g., section 9 of the *Charities Act 1993* which grants the Charity Commission the power to request 'any information' in someone's possession which relates to any charity."[33] The report noted the comments of Lord MacDonald QC, the former Director of Public Prosecutions, that "despite the enactment of RIPA, there remains 'a wealth of other statutes' under which public bodies may gain access to communications data."[34]

[33] Freedom from Suspicion: Surveillance Reform for a Digital Age, para 153
[34] *Ibid*