# The *Data Retention and Investigatory Powers Bill*

Standard Note: SN/HA/6934
Last updated: 16 July 2014
Author: Philip Ward
Section Home Affairs

---

On 10 July 2014 the Government announced that emergency legislation would be introduced on access to telecommunications data. The *Data Retention and Investigatory Powers Bill*, with accompanying Explanatory Notes, was published in draft on 10 July. The final Bill, with further accompanying documents, was published and given first reading on 14 July. All remaining Commons stages were set for 15 July. The Lords will consider it on the two following days and it will return to the Commons if necessary on 17 July for consideration of Lords amendments (if any).

The Government argues that emergency legislation is needed to ensure that UK law enforcement and intelligence agencies can maintain their ability to access the telecommunications data they need to investigate criminal activity and protect the public. There is cross-party agreement on the need for the Bill.

In April 2014, the European Court of Justice declared invalid a Directive enabling communication service providers to retain communications data for law enforcement purposes for periods of between six months and two years. This Directive has been transposed into UK law by way of secondary legislation. The Bill provides powers to replace those 2009 Regulations.

The ability to access content (rather than metadata) requires a warrant signed by a Secretary of State. The Bill amends the *Regulation of Investigatory Powers Act 2000* (RIPA) to put beyond doubt that requests for interception and communications data to overseas companies that are providing communications services within the UK are subject to the legislation.

At the same time the Prime Minister announced other measures, including a review of RIPA with a view to reforming and updating it, the establishment of a Privacy and Civil Liberties Oversight Board, annual "transparency reports" on the use of surveillance powers and a restriction on the number of public bodies able to request communications data.

This note summarises the background, the Bill and criticisms that have been made of it.

## Contents



## 1 Introduction

On 10 July 2014 the Government announced that emergency legislation would be introduced on access to telecommunications data. The resultant Bill was approved by a special Cabinet meeting and announced at a joint press conference by the Prime Minister and Deputy Prime Minister.

The *Data Retention and Investigatory Powers Bill* (Bill 73 2014-15), with accompanying Explanatory Notes, was published in draft on 10 July. The final Bill, with further accompanying documents,[1] was published and given first reading on 14 July. All remaining Commons stages were set for 15 July.[2] The House of Lords will consider it on the two following days and it will return to the Commons if necessary on 17 July for consideration of Lords amendments (if any).

The stated context for the Bill is the continuing threat from serious organised crime and the growing threat from international terrorism. The Government argues that emergency legislation is needed to ensure that UK law enforcement and intelligence agencies can maintain their ability to access the telecommunications data they need to investigate criminal activity and protect the public. This has cross party agreement.

The Government says that it is taking this action following two recent developments. First, the European Court of Justice (ECJ) has struck down regulations enabling communication service providers (CSPs) to retain communications data for law enforcement purposes for a specified period. The Government is concerned that, unless they have a business reason to hold this data, internet and phone companies, fearing legal action, will start deleting it. This

---

1 Explanatory Notes, Impact assessments and draft secondary legislation - *Provisional draft of the Data Retention Regulations 2014*. There was no difference between the texts of the draft and final Bill.

2 HC Deb 15 July 2014 cc682-834

could have serious consequences for investigations – investigations which can take many months and which rely on retrospectively accessing data for evidential purposes.

Secondly, some companies are calling for a clearer legal framework to underpin their cooperation with law enforcement and intelligence agencies to intercept what terrorists and serious criminals are saying to each other. This is the ability to access content with a warrant signed by a Secretary of State.[3]

Following the Cabinet meeting, the Prime Minister and Deputy Prime Minister gave a joint press conference. Mr Cameron said that his main priority was national security:

> "As events in Iraq and Syria demonstrate, now is not the time to be scaling back on our ability to keep our people safe. No government introduces fast-track legislation lightly. But the consequences of not acting are grave."[4]

Mr Clegg insisted that the emergency Bill was not the prelude to a reintroduction of the controversial *Communications Data Bill*, the so-called "snooper's charter", which was opposed by the Liberal Democrats and subsequently dropped. That Bill would have required companies to keep records for at least a year of every website visited by a subscriber.[5] "Liberty and security must go hand in hand", he told the conference. "We can't enjoy our freedoms if we don't have the capability to keep ourselves safe". Both leaders stressed that the new Bill did not, in their view, represent an extension of the state's powers, merely a restoration of the *status quo ante*. However, the Government cannot predict, in a fast-changing environment, what will happen after the next Election. In the words of the Explanatory Memorandum:

> 32… This Bill does not enhance data retention powers, although it is envisaged that when communications data policy is considered in the next Parliament, legislation conferring further powers may be proposed.

The Home Secretary made a statement to the Commons on the same day. Mrs May reiterated the points made by the Prime Minister. Without this legislation, she said,

> we face the very prospect of losing access to this data overnight, with the consequence that police investigations would suddenly go dark and criminals would escape justice. We cannot allow that to happen. (…)
>
> In the face of such a diverse range of threats, the Government would be negligent if they did not make sure the people and the organisations that keep us safe—the police, other law enforcement agencies and the security and intelligence agencies—have the legal powers to utilise the capabilities they need. They are clear that we need to act immediately. If we do not, criminals and terrorists will go about their work unimpeded, and innocent lives will be lost.[6]

Responding to the statement, Yvette Cooper, shadow Home Secretary, indicated that the measures had Opposition support, albeit with reservations:

---

3 Summary of the Government's position taken from: Prime Minister's Office press release, *PM and Deputy PM to announce emergency security legislation*, 10 July 2014

4 "UK unveils emergency data law to underpin security surveillance", *Financial Times*, 10 July 2104

5 On this, now abandoned, draft legislation, see an earlier House of Commons Library Note: *Communications data: the draft Bill and recent developments*, SN6373, May 2013

6 HC Deb 10 July 2014 cc457, 459

> We agree with the Home Secretary that a temporary and urgent solution is needed as a result of the European Court judgment in April, because otherwise the police and intelligence agencies will suddenly lose vital information and evidence this summer. It would be too damaging to the fight against serious and organised crime, to the work against online child abuse, and to counter-terror investigations to risk losing that capability over the next two months while Parliament is in recess, and that is why we need to act.
>
> However, as the Home Secretary will appreciate, there will be serious concern, in Parliament and throughout the country, about the lateness of this legislative proposal, and about the short time that we have in which to consider something so important. That lack of time for debate makes the safeguards that we have discussed particularly important, and I want to press the Home Secretary on some of them. It also makes it essential for the Government to engage in a wider, public debate about how we balance privacy and security in an internet age.[7]

Sir Bernard Hogan-Howe, Metropolitan Police Commissioner, was quoted as saying:

> "All we're trying to do is to maintain the level of surveillance that we've already got… If we lose it – and there's some danger that we already losing it – then we will all be less safe."[8]

## 2 The value of communications data

The Explanatory Notes to the Bill summarise what is meant by "communications data":

> 7. Communications data is the context not the content of a communication. It can be used to demonstrate who was communicating; when; from where; and with whom. It can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It does not include the content of any communication: for example the text of an email or a conversation on a telephone.

According to a statement from the Prime Minister's Office, communications data of this kind has been used in 95% of all serious organised crime cases handled by the Crown Prosecution Service. It has been used in every major Security Service counter-terrorism investigation over the last decade. It is particularly important for targeting serious criminals, including drug dealers, paedophiles and fraudsters. It has also been used to stop crimes in action and save lives, and to prevent miscarriages of justice. The statement includes a number of examples of successful prosecutions mounted using mobile phone call and text evidence. Whilst conceding that it is difficult to be definitive about the impact of *not* requiring companies to retain this data, the statement quotes a recent Europol investigation into online child sexual exploitation (known as Operation Rescue) which gives an indication of what the impact would be:

> Of 371 suspects identified in the UK, 240 cases were investigated and 121 arrests or convictions were possible. One man was sentenced in March 2010 to 6 years' imprisonment for sexual abuse of 2 minors after police discovered more than 60,000 indecent images on his computer.
>
> In contrast, of 377 suspects identified in Germany, which has no such data retention arrangements, only 7 could be investigated and no arrests were made.[9]

---

7 HC Deb 10 July 2014 c459
8 *Guardian*, 11 July 2014, p7

A memorandum from the European Commission justifies the value of data retention for criminal justice systems and law enforcement:

> Data retention takes place in most Member States. Member States have generally reported that retained data is very valuable, and in some cases indispensable, for preventing and combating crime, for protecting victims and for the acquittal of the innocent in criminal cases.
>
> The evidence, in the form of statistics and examples provided by Member States, is limited in some respects but nevertheless attests to the very important role of retained data for criminal investigation. This data provides valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Its use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons.
>
> Data retention enables the construction of trails of evidence leading up to an offence. It also helps to discern or corroborate other forms of evidence on the activities of and links between suspects and victims. In the absence of forensic or eye witness evidence, data retention is often the only way to start a criminal investigation. Generally, data retention appears to play a central role in criminal investigation even if it is not always possible to isolate and quantify the impact of a particular form of evidence in a given case. [10]

## 3 The Data Retention Directive

EC Directive 2006/24/EC, introduced in the wake of the Madrid bombings and the "7/7" attacks in London, imposes obligations on electronic communications businesses to retain data generated by them for billing purposes for periods of between six months and two years. Individual Member States can set their own retention periods within those parameters. Telecommunication service providers are required to make their stored traffic and location data available on request to law enforcement authorities for the purpose of investigation, detection and prosecution of serious crime and terrorism.

The memorandum from the European Commission explains which types of data are currently being retained under the Directive:

> The Directive requires telecommunications service providers to retain (store) traffic and location data generated or processed by service and network providers as a result of communications activities. It does not require or allow the retention of the content of the communications (it is therefore different from lawful interception or 'wiretapping'). The Data Retention Directive applies to the fields of fixed network telephony, mobile telephony, internet access, internet email and internet telephony. It requires service providers to retain those traffic data necessary for identifying the source (i.e. sender), destination (recipient), date, time and duration, type, equipment of communication, and, for mobile telephony, the location of the equipment.

## 4 Transposition of the Directive into UK law

A voluntary Code of Practice on the Retention of Communications Data has 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

---

9 Prime Minister's Office press release, *PM and Deputy PM to announce emergency security legislation*, 10 July 2014

10 European Commission memo, *Frequently asked questions: the Data Retention Directive*, Memo/14/269, 8 April 2014

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*.

In August 2008 the last Government published a consultation paper on the transposition of Directive 2006/24/EC.[11] This Directive mandates the retention, by public communications providers (e.g. telephone companies), of communications data. An initial transposition – covering only fixed line and mobile telephony – was effected by the *Data Retention (EC Directive) Regulations* SI 2007/2199. The above-mentioned consultation proposed the revocation of these regulations and their replacement by the *Data Retention (EC Directive) Regulations 2009* SI 2009/859. These newer regulations complete the transposition of the EC Directive by extending the application of communications data retention measures to include internet access, internet telephony and email as well as the, already covered, fixed line and mobile telephony data. The retention of data is now mandatory (for twelve months) while the reimbursement of costs remains as under the voluntary system. The Directive was careful to note that communication service providers were not being required to collect information that they do not already collect.

In its response to the consultation on transposition, Liberty drew attention to the interaction of data protection law and the *Human Rights Act 1998*:

> 4. At paragraph 2.7 the consultation states that business will be able to retain data for periods over the minimum 12 months so long as the Data Protection Act 1998 (DPA) is complied with. While it is correct to refer to the DPA it is also necessary, we would also suggest that retention periods would also need to be compatible with the Human Rights Act 1998. Although communications data providers are not public authorities any private body carrying out a public function is covered by the HRA. If the purpose of communications data retention is for national security, crime detection/prevention and so on then we suggest that those holding the data will be carrying out a public function. In practical terms there will not be a significant distinction between DPA compliance and HRA compliance. Many of the data protection principles, such as only processing data for legitimate purposes and not retaining data for longer than necessary, mirror HRA requirements for proportionality and necessity. However in terms of presentation, it is important to acknowledge that all those who hold communications data do so in accordance with human rights principles.[12]

A schedule to the 2009 regulations details the communications data that must be retained (any unconnected calls are not covered). For example, in the context of fixed network telephony, the following is 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.

---

[11] Home Office, *A consultation paper: transposition of Directive 2006/24/EC*, August 2008

[12] Liberty, *Response to the Home Office consultation paper: transposition of Directive 2006/24/EC*, October 2008

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

An important caveat to the above is 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.

Transposition of the Directive into national law has proved problematic in several EU countries. The Commission memorandum offers a summary:

> Constitutional courts in several Member States (Germany, Romania, the Czech Republic and to some extent Cyprus and Bulgaria) found national data retention laws to be unconstitutional. In no case did the courts rule that the Data Retention Directive is contrary to fundamental rights.
>
> The German Constitutional Court did not consider data retention unconstitutional as such, but found the law transposing the Directive to be unconstitutional since it did not sufficiently limit the circumstances in which law enforcement authorities could access the data, and did not contain sufficient measures to protect retained data against breaches of confidentiality (data security).
>
> The Romanian Court found the law transposing the Directive to be ambiguous in its scope and purpose, with insufficient safeguards, and found, against that background, the obligation to retain data for a period of six months to be unconstitutional.
>
> The Czech Constitutional Court annulled the law transposing the Directive on the basis that, as a measure which interfered with fundamental rights, it was insufficiently precise and clear in its formulation.
>
> Of these Member States only Germany so far has failed to transpose in a way that complies with its respective national court judgment.

In her statement to the Commons, the Home Secretary suggested that it might have been preferable if the UK had implemented the Directive through primary legislation:

> The ECJ judgment clearly has implications not just for the United Kingdom, but for other EU member states, and we are in close contact with other European Governments. Other countries, such as Ireland and Denmark, implemented the data retention directive through primary legislation, which means they have retained a clear legal basis for their data retention policies, unless a separate, successful legal challenge to their legislation is made. The UK does not have that luxury, because here the data retention directive was implemented through secondary legislation.[13]

## 5 The ECJ judgment

In a judgment on 8 April the Court of Justice of the EU (ECJ) declared the EU Data Retention Directive invalid.[14] The ruling supported the earlier Opinion of Advocate General, Cruz Villalon, in December 2013, who found the Directive incompatible with the EU's Charter of Fundamental Rights. The case was bought by the High Court in Ireland and the Constitutional Court in Austria, who asked the ECJ to examine the validity of the Directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of

---

13 HC Deb 10 July 2014 c457

14 Joined cases C-293/12 and C594/12, Digital Rights Ireland and Seitlinger and Others. See Court press release, 8 April 2014 and Commission press release, 8 April 2014.

the EU, namely the right to respect for private life and the right to the protection of personal data.

The Court concluded that, in adopting the Data Retention Directive, "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality".[15] It held the Directive to be in breach of Articles 7 and 8 of the EU Charter of Fundamental Rights and Freedoms as well as Article 8 of the European Convention on Human Rights. The ECJ determined that the Directive represents a serious interference with these fundamental rights without limiting that interference to what is strictly necessary. In particular, the Court found as follows:

> Firstly, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without **any differentiation, limitation or exception** being made in the light of the objective of fighting against serious crime.
>
> Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have **access to the data** and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.
>
> Thirdly, so far as concerns **the data retention period**, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.
>
> The Court also finds that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the **risk of abuse** and against any unlawful access and use of the data. It notes, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period. www.curia.europa.eu
>
> Lastly, the Court states that the directive does **not** require that the data be **retained within the EU.** Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[16]

A footnote to the Court's press release states that "given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on

---

[15] Para 69 of the full judgment available on the Curia website

[16] ECJ press release, 8 April 2014

which the directive entered into force". In other words, the Directive is invalid with immediate effect.

The Court's judgment is lengthy and complex. Analysts who have studied it closely have suggested that it can be broken down into ten "principles". Any legislation mandating data retention by an EU Member State must, on this analysis, comply with the following principles:

> 1. restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);
>
> 2. provide exceptions for persons whose communications are subject to an obligation of professional secrecy (paragraph 58);
>
> 3. distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
>
> 4. ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);
>
> 5. empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);
>
> 6. restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);
>
> 7. limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);
>
> 8. ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access (paragraph 66);
>
> 9. ensure destruction of the data when it is no longer required (paragraph 67); and
>
> 10. ensure the data is kept within the EU (paragraph 68).[17]

As the case in question was a Preliminary Ruling, made at the request of the Irish and Austrian courts, the ruling given by the ECJ is first and foremost for the purposes of being applied by those particular national courts to resolve the domestic disputes before them (i.e. domestic claims that relevant domestic implementing legislation is invalid). However, it is generally accepted that preliminary rulings have to be followed by all Member State courts in similar cases. The UK Government is concerned that, without new legislation, data could be destroyed within weeks by communication service providers fearing legal challenges, with the result that the police and security services would be unable to access it.[18]

## 6 A domestic legal challenge

Now that the EC Directive has been transposed into UK law, what is the effect of the ECJ judgment on existing UK legislation? The European Commission memorandum observes:

---

[17] Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN, *Briefing on the fast-track Data Retention and Investigatory Powers Bill*, 14 July 2014

[18] "Emergency phone and internet data retention law to be passed", *BBC News*, 10 July 2014. On this point, the *Guardian* reports that "communication service providers said they did not know of any companies that had warned the UK government they would start deleting data in light of the legal uncertainty" ("Cameron makes concessions to rush through snooping law", *Guardian*, 11 July 2014, pp1, 6)

> National legislation needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the European Court of Justice. Furthermore, a finding of invalidity of the Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data.

Following the judgment, the Government advised communications providers to carry on retaining data as required under the 2009 Regulations:

> **Dr Huppert:** To ask the Secretary of State for the Home Department with reference to the answer of 28 April 2014, *Official Report,* column 437W, on telecommunications: databases, whether she has yet completed her assessment of *(a)* the consequences for the UK of the decision of the European Court of Justice in Joined Cases C-293/12 and C-594/12 (Digital Rights Ireland and Seitlinger and Others) and *(b)* what implication that decision has for (i) enforcement of the Data Retention (EC Directive) Regulations 2009 and (ii) her powers to reimburse any expenses incurred by a public communications provider in complying with those regulations. [199250]
>
> **James Brokenshire:** The Government continues to consider the judgment of the European Court. At the present time, we consider that the UK Data Retention (EC Directive) Regulations 2009 remain in force. Those in receipt of a notice under the regulations have been informed that they should continue to observe their obligations as outlined in any notice.[19]

There is an ongoing challenge in the British courts to the legality of the 2009 Regulations in the form of a judicial review originally lodged by Tracey Cosgrove in 2011.[20] The proceedings challenge the legality of the 2009 Regulations and in particular their compatibility with Article 8 of the ECHR and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The judicial review also alleges that the Regulations are *ultra vires* the *European Communities Act 1972*. The Claimant is seeking an order quashing the Regulations.

The judicial review was initially stayed pending the outcome of the ECJ judgment. The Home Secretary has now confirmed that she has notified the High Court of the ECJ judgment. The judicial review claim will therefore proceed. If the judicial review is successful, the UK Regulations would be declared unlawful by a UK court. Any new regulations could also be subject to judicial review if they do not comply with the ECJ judgment.[21]

## 7 RIPA

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).

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. Hence the importance attached to the *retention* of data.

---

19 HC Deb 166 June 2014 c445W. For responses to this answer from campaigning groups, see "British government 'breaking law' in forcing data retention by companies", *Guardian*, 24 June 2014.

20 *Tracey Cosgrove v Secretary of State for the Home Department*, CO/7701/2011

21 Open Rights Group, *Briefing to MPs on data retention legislation*, 9 July/14 July 2014

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.[22]

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;
>
> (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.[23] 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.[24]

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.

---

22 http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

23 The most recent order, superseding three earlier ones, is the *Regulation of Investigatory Powers (Communications Data) Order* SI 2010/480

24 http://www.official-documents.gov.uk/document/hc0708/hc02/0252/0252.asp (HC 252)

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.

A House of Commons Library Note looks at past and present law in this area and the role of the Interception of Communications Commissioner in overseeing the present regime.[25]

## 8 The Bill

The emergency Bill falls into two parts. The first, "Retention of relevant communications data", provides powers to replace the 2009 Regulations, which have been declared invalid by the ECJ. Specifically **–**

**Clause 1(1)** provides power for the Secretary of State to issue a data retention notice on a telecommunications services provider, requiring them to retain certain data types. The data types are those set out in the Schedule to the 2009 Regulations. No additional categories of data can be retained. Clause 1(1) creates the additional safeguard that the Secretary of State must consider whether it is "necessary and proportionate" to give the notice for one or more of the purposes set out in s22(2) of RIPA. These purposes, which are the same purposes for which retained data can be accessed under RIPA

**Clause 1(2)** lists the issues a notice may cover. A notice cannot require the retention of data types other than those that were required to be retained by the 2009 Regulations, but may limit the requirement to a subset of these data types where appropriate.

**Clause 1(3)** allows for the Secretary of State to make regulations relating to the retention of relevant communications data. These regulations will replace the 2009 Regulations.

**Clause 1(4)** gives examples of the matters that may be provided for in the regulations. These include further provision on the giving of and contents of notices, safeguards for retained data, enforcement of requirements relating to retained data and the creation of a code of practice in order to provide detailed guidelines for data retention and information about the application of safeguards. The regulations may also provide for the revocation of the 2009 Regulations, and transitional provisions.

**Clause 1(5)** provides that the period for which data can be retained can be set at a maximum period not to exceed 12 months, rather than the fixed 12 months in the 2009 Regulations, allowing for retention for shorter periods when appropriate.

**Clause 1(6)** specifies that data retained under the provisions in this legislation can only be acquired through Chapter 2 of Part 1 of RIPA, through an order of the court or other judicial warrant or authorisation, or as specified in regulations made under subsection (3).

**Clause 2** provides a number of relevant definitions of terms to clarify who and what is caught by the Bill. **Clause 2(5)** specifies that any statutory instrument laid under clause 1 will be subject to the "affirmative resolution" procedure.[26]

---

[25] *Interception of communications*, SN/HA/6332, May 2012

[26] Meaning that it does not become law unless a draft of the instrument has been laid before, and approved by a resolution of, both Houses of Parliament.

The second part of the Bill, "Investigatory powers", comprises three clauses which amend RIPA.

**Clause 3** amends s5 of RIPA regarding the Secretary of State's power to issue interception warrants on the grounds of economic well-being. The *Code of Practice for the Interception of Communications*, made under s71 of RIPA, specifies that interception warrants can only be issued on such grounds when economic well-being is directly related to national security. This detail is now included on the face of the Bill. The clause makes a similar amendment with respect to access to communications data. The *Code of Practice for the Acquisition and Disclosure of Communications Data*, made under s71 of RIPA, specifies that data can only be acquired in the interests of the economic well-being of the United Kingdom when it specifically relates to national security. This detail is now is included on the face of the Bill.

**Clause 4** aims to clarify the extra-territorial reach of RIPA in in relation to both interception and communications data by adding specific provisions. This confirms that requests for interception and communications data to overseas companies that are providing communications services within the UK are subject to the legislation. The Explanatory Notes give background to this amendment:

> 15… While RIPA has always had implicit extraterritorial effect, some companies based outside the United Kingdom, including some of the largest communications providers in the market, have questioned whether the legislation applies to them. These companies argue that they will only comply with requests where there is a clear obligation in law. When RIPA was drafted it was intended to apply to telecommunications companies offering services to United Kingdom customers, wherever those companies were based. It is now important to make that clear on the face of the legislation.

The current definition of "telecommunications service" contained in RIPA states that:

> "telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)[27]

A "telecommunications system" is defined broadly as any system for facilitating communications electronically. **Clause 5** clarifies the definition of "telecommunications service" in RIPA to ensure that internet-based services, such as webmail, are included in the definition.[28]

**Clause 6** states that the Bill extends to the whole of the United Kingdom and will come into force on the day in which it is passed. Subsection (3) is a so-called 'sunset clause', providing that the entire Act (and therefore the amendments made to RIPA by this Act) will be repealed at the end of 2016.

## 9 Criticism of the Bill

Jim Killock, executive director of the Open Rights Group, accused the Government of "using the threat of terrorism as an excuse" for passing fast-track legislation when it suited their purposes. He said:

> "Not only will the proposed legislation infringe our right to privacy, it will also set a dangerous precedent where the Government simply re-legislates every time it

---

27 *Regulation of Investigatory Powers Act 2000* s2(1)

28 The potentially wide scope of this definition has already provoked debate (see: "Secret expansion of spying despite Coalition's pledge", *Sunday Times*, 13 July 2014, p8)

> disagrees with a decision by the ECJ. The ruling still stands and these new plans may actually increase the amount of our personal data that is retained by ISPs, further infringing on our right to privacy. Blanket surveillance needs to end. That is what the court has said."[29]

Since the April ruling, campaigners have reportedly been applying pressure on communications companies to stop retaining their data. More than 1,500 letters were sent to companies by campaigners, the Open Rights Group told the BBC. The letters threatened to take further action unless their data was deleted and no longer collected, citing the European court decision as justification. While no communications companies are understood to have deleted any data, it is understood the firms were pressing the government to act quickly to clarify the law. The Open Rights Group has not launched legal action against communication firms, but it had signalled its intention to report the companies to the Information Commissioner's Office.[30]

Questions have been raised about the timing of the Bill's introduction, falling as it has shortly before the Commons and Lords rise for the summer recess. Critics have pointed out that although the ECJ ruling occurred three months ago, Members will have little time to scrutinise the Bill in detail. Tom Watson MP has described the Bill as a "stitch-up" and "secret deal between party leaders". [31]

Shami Chakrabarti, Director of Liberty, said:

> "The Government says it's only plugging loopholes but its existing blanket surveillance practice has been found unlawful.
>
> "We are told this is a paedophile and jihadi 'emergency', but the court judgment they seek to ignore was handed down over three months ago and this isn't snooping on suspects but on everyone.
>
> "We are promised greater scrutiny and debate but not until 2016, as it seems that all three party leaders have done a deal in private. No privacy for us and no scrutiny for them.
>
> "Will Clegg and Cameron's 'debate for the future' really comfort voters and companies today?"[32]

A question on the lips of sceptical observers is: to what extent does the emergency Bill comply with the principles established by the ECJ decision? The legal commentator Graham Smith has a table on his blog listing the ECJ's specific grounds for invalidating the Data Retention Directive and considering how, on his reading, the Bill does or does not address

---

29 Quoted in: "Emergency data law: Government 'railroading' through legislation on internet and phone records", *Independent*, 10 July 2014

30 "What emergency data law means for you", *BBC News*, 10 July 2014. The Information Commissioner regulates the implementation of data protection law.

31 "Emergency data law: Government 'railroading' through legislation on internet and phone records", *Independent*, 10 July 2014

32 Liberty press release, *Emergency data law: a "debate for the future"?* 10 July 2014

them.[33] A number of civil liberties groups joined forces to publish a joint briefing for MPs and others on the eve of the parliamentary debate. [34]

## 10 Further steps

The statement from the Prime Minister's Office announced further steps, in addition to the new legislation, to "strengthen oversight and transparency":

- the Bill includes a termination clause that ensures the legislation falls at the end of 2016 and the next government is forced to look again at these powers
- between now and 2016 we will hold a full review of the Regulation of Investigatory Powers Act, to make recommendations for how it could be reformed and updated
- we will appoint a senior diplomat to lead discussions with the American government and the internet companies to establish a new international agreement for sharing data between legal jurisdictions
- we will establish a Privacy and Civil Liberties Oversight Board on the American model, to ensure that civil liberties are properly considered in the formulation of government policy on counter-terrorism. This will be based on David Anderson's existing role as the Independent Reviewer of Terrorism Legislation.
- we will restrict the number of public bodies that are able to approach phone and internet companies and ask for communications data. Some bodies will lose their powers to access data altogether while local authorities will be required to go through a single central authority who will make the request on their behalf.
- finally, we will publish annual transparency reports, making more information publicly available than ever before on the way that surveillance powers operate.[35]

## 11 Commons amendments on 15 July

In the Commons the Bill was considered by a Committee of the Whole House immediately after second reading on 15 July. Amendments were tabled during the day. Some were amendments to existing clauses, some were additional clauses. Of the amendments tabled, there seem to have been four New Clauses (NCs) of significance for the Bill's progress:

**NC1** (tabled by the Opposition) provided for a review of the powers, regulations, proportionality and oversight for communications and interception. This review was to be begin "as soon as practicable".

**NC2** (tabled by the Opposition) required the Interception of Communications Commissioner to report on the operation of the new Act within six months of its coming into force and at six-monthly intervals thereafter.

---

33 http://www.cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html. Mr Smith describes himself on his blog as a "private practice lawyer based in London, England, dealing with IT, internet and intellectual property issues".

34 Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN, *Briefing on the fast-track Data Retention and Investigatory Powers Bill*, 14 July 2014

35 Prime Minister's Office press release, *PM and Deputy PM to announce emergency security legislation*, 10 July 2014

**NC6** (tabled by the Opposition) required the Interception of Communications Commissioner to report to Parliament on the operation of RIPA at six-monthly intervals, instead of annually as at present.

**NC7** (tabled by the Government) provided for a review of investigatory powers and their regulation, to be completed, "as far as reasonably practicable", before 1 May 2015. This puts on the face of the Bill a commitment which the Prime Minister made when the Bill was first announced (albeit with a tighter timescale).

The Government accepted NC6 and invited the Opposition to withdraw NC2.[36] The Opposition said, in response, that they would support NC7, "which meets our objectives".[37] David Hanson, shadow minister, explained that a compromise had been reached:

> The Opposition had two objectives in tabling our amendments and new clauses today: first, to secure a review of this Act, if passed by this House and by the House of Lords, within six months and then every six months following that; and secondly, to put it on the record that we need to have a wider examination of the whole of the intercept evidence-data collection issue. I think we have had a meeting of minds on that issue.[38]

An amendment to the 'sunset clause' in the name of Tom Watson was intended to bring the Act to an end in 2014. This was defeated by 454 votes to 56.[39] The Bill was passed on third reading by 449 votes to 33[40] and moved to the Lords on 16 July.[41]

---

36 The Minister, James Brokenshire, at HC Deb 15 July 2014 c805
37 David Hanson at HC Deb 15 July 2014 c807
38 HC Deb 15 July 2014 c807
39 HC Deb 15 July 2014 c807
40 HC Deb 15 July 2014 c830
41 As HL Bill 37 2014-15