HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 7371, 19 November 2015

Draft Investigatory Powers Bill

By Joanna Dawson

Inside:

Contents

Summary

The *Draft Investigatory Powers Bill* was published by the Home Office on 4 November 2015. It seeks to update and consolidate existing legislation governing the use of investigatory powers, including the *Regulation of Investigatory Powers Act 2000*.

The Draft Bill follows the publication in 2015 of three significant reports on investigatory powers, by the Government's independent reviewer of terrorism legislation; the Royal United Services Institute; and the Intelligence and Security Committee. All three reports concluded that the current framework was outdated, unworkable and in need of reform. They highlighted the need for greater transparency, more stringent safeguards and better oversight.

A previous attempt to reform this area of law, the *Draft Communications Data Bill 2012*, was abandoned under the Coalition Government as a result of differences between the Conservatives and the Liberal Democrats. The Draft Bill replicates a number of measures put forward in the *Draft Communications Data Bill*, but some of the more controversial proposals have been left out.

The Draft Bill makes provision for the issue of warrants for interception and equipment interference and for authorisations in relation to the acquisition of communications data. For the first time it requires that warrants should be subject to judicial, as well as ministerial, oversight. It also reforms the current oversight framework and provides for a right of appeal from the Investigatory Powers Tribunal.

The initial political response to the Draft Bill was generally positive, particularly with respect to greater transparency and the opportunity for full parliamentary consideration of the issues. However, concerns have been raised as to the breadth of the powers sought by the intelligence agencies, and the sufficiency of the safeguards.

1. Introduction

The *Draft Investigatory Powers Bill* was published by the Home Office on 4 November 2015.[1] Presenting the Bill to Parliament, Theresa May said that it would consolidate and update investigatory powers, strengthen safeguards and establish a world-leading oversight regime:

> This Bill will govern all the powers available to law enforcement, the security and intelligence agencies and the armed forces to acquire the content of communications or communications data. These include the ability to retain and acquire communications data to be used as evidence in court and to advance investigations; the ability to intercept the contents of communications in order to acquire sensitive intelligence to tackle terrorist plots and serious and organised crimes; the use of equipment interference powers to obtain data covertly from computers; and the use of these powers by the security and intelligence agencies in bulk to identify the most serious threats to the UK from overseas and to rapidly establish links between suspects in the UK.[2]

On 5 November the House of Commons agreed a resolution that a Joint Select Committee should be appointed to consider and report on the Draft Bill. The Commons members were announced as Victoria Atkins, Suella Fernandes, David Hanson, Stuart C McDonald, Dr Andrew Murrison, Valerie Vaz and Matt Warman.[3]

The Government intend that legislation should be in place by the end of 2016.[4]

The Draft Bill extends to the whole of the United Kingdom. However, it may be necessary to obtain legislative consent motions with respect to certain aspects of the Bill which impinge on matters devolved to the Scottish Parliament, including the investigation of serious crime and the signing of warrants relating to law enforcement.[5]

This Briefing Paper provides an overview of the provisions contained in the Bill and of the recommendations made in the three reports on investigatory powers. Not all clauses are covered individually. Clauses that are technical or self-explanatory are not addressed.

---

[1] Draft Investigatory Powers Bill, Cm 9152, November 2015
[2] HC Deb 4 November 2015, c 969-972
[3] HC Deb 5 November 2015, c1227
[4] HC Deb 19 October 2015, c709
[5] HC Deb 4 November 2015, c979

2. Background

Legislative framework

The *Regulation of Investigatory Powers Act 2000* (RIPA) contains much of the existing legal framework governing the powers of the intelligence and law enforcement agencies to intercept communications in order to access their content, and to acquire communications data. The Act provides for a scheme of warrants and oversight which was intended to be comprehensive and compliant with the European Convention on Human Rights (ECHR).

When RIPA was introduced the then Home Secretary Jack Straw described it as an "important bill, and … a significant step forward for the protection of human rights in this country".[6] However, the Act has been the subject of persistent criticism, focusing on the arcane and inaccessible style in which it was drafted. Furthermore, since RIPA came into force, methods of communicating, and the volume of communications data potentially available, have increased significantly. There now exists a broad consensus that the legislative framework is in need of modernisation and clarification.

In addition to RIPA a number of other statutes also allow for the interception of communications and the acquisition of communications data. These include the *Wireless Telegraphy Act 2006*, the *Telecommunications Act 1984*, the *Police and Criminal Evidence Act 1984* and the *Terrorism Act 2000*. The *Intelligence Services Act 1994* gives the Secretary of State the power to issue warrants authorising MI5, MI6 and GCHQ to interfere with property. The Government has recently acknowledged that this power is used to authorise equipment interference, also known as hacking.

RIPA does not regulate what data must be retained, dealing only with acquisition and disclosure. Therefore when RIPA was introduced, the only data available to be accessed was the data retained by Communications Service Providers (CSPs) for their own purposes. In 2005 the EU adopted the Data Retention Directive,[7] requiring the mandatory retention of data on communication networks. The UK transposed the directive into national law via the Data Retention Regulations.

In 2009 the Labour Government consulted on a plan to legislate to compel CSPs based in the UK to collect and keep all data public authorities might need, including third party data crossing their networks, and to make all this data accessible on a case-by-case basis to public authorities.[8] No legislation was put forward before the 2010 general election.

Interception
Interception is defined as making available the content of a communication – such as a telephone call, email or social media message – in the course of its transmission or while stored on a telecommunications system

Communications data
Communications data is described as information about communications, the 'who', 'where', 'when', 'how', and 'with whom' but not what was written or said

[6] HC Deb 6 March 2000, c 767
[7] 2006/24/EC
[8] Protecting the Public in a Changing Communications Environment, Home Office, April 2009

In June 2012 the coalition Government published the *Draft Communications Data Bill.* The Bill, which was dubbed the "Snoopers' Charter" by critics due to the breadth of the powers sought, would have replaced those parts of RIPA that deal with the acquisition of communications data. It proposed significantly extending the range of data CSPs have to store. It would have included for the first time records of each user's internet browsing activity (websites visited but not pages within websites), details of messages sent on social media, webmail, voice calls over the internet, and gaming, in addition to emails and phone calls.

A number of bodies would have had access to this data, namely: the Police, the Serious and Organised Crime Agency, the intelligence agencies and HM Revenue and Customs. Access would not have been subject to judicial authorisation, provided it was required for the purpose of investigating crime or protecting national security.

The Government believed that the Bill was necessary in order for the police and intelligence and security agencies to operate effectively in a fast-changing environment of communications technology, in which far more communications take place over the internet.

A Joint Committee set up to scrutinise the Bill reported in December 2012. The Committee concluded that the powers to order the retention of data contained in the Bill should be significantly narrowed, and safeguards against abuse introduced, before it could be workable. It also recommended that there should be much better consultation with industry, technical experts, civil liberties groups, public authorities and law enforcement bodies before a new Bill was introduced.[9]

The Intelligence and Security Committee also published a report raising similar concerns, including that there had been insufficient consultation with CSPs.[10]

Following publication of these reports it became apparent that the issue was becoming increasingly contentious, and the draft Bill did not proceed.

In 2014 the issue was reignited when the Court of Justice of the European Union (CJEU) declared the Data Retention Directive invalid, on the basis that it infringed privacy and data protection rights guaranteed by the European Union Charter of Fundamental Rights.[11] In the absence of a framework requiring the retention of communications data by service providers, the ability of law enforcement agencies to access that data would be impeded. Therefore, the Government fast-tracked the *Data Retention and Investigatory Powers Act 2014* (DRIPA) in order to recreate a regime that would ensure that data was retained.

---

[9] Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill*, 11 December 2012, HL Paper 79, HC 479

[10] Intelligence and Security Committee, Access to communications data by the intelligence and security Agencies, Cm 8514, 5 February 2013

[11] Digital Rights Ireland C-293/12

A subsequent judicial review of DRIPA, brought by MPs David Davis and Tom Watson, found that section 1 was incompatible with EU law, as interpreted by the CJEU.[12] Section 1 allows the Home Secretary to issue a retention notice to a service provider requiring them to retain communications data where the requirement is necessary and proportionate for a purpose falling under RIPA. The effect of the judgment, which would be to invalidate the provision in question, was suspended until March 2016 in order to give the Government the opportunity to put alternative measures in place. The Government are in the process of appealing the decision, but regardless of the outcome of that appeal, alternative measures would in any event be required by the end of 2016, due to a sunset clause in DRIPA.

Part 3 of the *Counter-Terrorism and Security Act 2015* (CTSA) amended DRIPA 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 internet protocol (IP) address at any given time.

Box 1: IP address resolution

An Internet Protocol (IP) address is a numerical label that acts much like an address for a computer on the Internet, allowing data to be delivered to that computer. Every device requires an IP address to be able to request and receive content from websites. These IP addresses can be recorded by website operators.

CSPs providing connections assign IP addresses to computers as and when they connect to the internet. The public IP address you are allocated by your CSP may be permanent (static) or temporary (dynamic). Businesses tend to have static addresses, whilst individuals tend to be assigned a dynamic address. This means an individual's IP address can change frequently.

CSPs have a limited number of IP addresses available that can be assigned at any one time—there may be 20,000 IP addresses and 40,000 customers. Since not everyone is connected at the same time, the CSP assigns a different IP address to each computer that connects, and reassigns it when they disconnect. Because of this, the IP address assigned to your computer one day may get assigned to several other computers (and different users) before a week has passed. Furthermore, if you share your computer or even just your connection to your ISP, then multiple people are sharing one IP address.

IP resolution is the ability to identify who was using an IP address. Identifying individuals using nothing more than their IP address has become a key part of anti-piracy and criminal investigations. This is possible if the data is available, however, there are a number of difficulties in identifying individuals from their IP address, including:

- IP addresses are shared by a number of users simultaneously and a CSP can usually only provide details of the person who pays the internet subscription. This is not necessarily the person who was using a device at a particular time.
- Some CSPs, particularly, those using dynamic IP addresses such as mobile phone operators, require destination IP as well as sender IP to match up who is involved in an action.

Reports on Investigatory Powers

The Anderson Report: *A Question of Trust*

Section 7 of DRIPA required the Government's independent reviewer of terrorism legislation, David Anderson QC, to conduct a review of the operation and regulation of investigatory powers, with specific reference to the interception of communications and communications data. The outcome of this review, A Question of Trust ("the Anderson

[12] *Davis et al v SSHD* [2015] EWHC 2092

Report"), was published on 11 June 2015.[13] It made extensive and detailed recommendations for a new legislative framework to replace RIPA and DRIPA. Key recommendations included:

- RIPA and related legislation should be replaced with a new law that would be both comprehensive and comprehensible.
- Security and intelligence agencies should have powers to carry out "bulk collection" of intercepted material but there must be "strict additional safeguards".
- Judges should authorise requests to intercept communications, limiting the Home Secretary's current role in deciding which suspects are so monitored.
- The definition of communications data should be reviewed, clarified and brought up to date.
- Oversight should be provided by an Independent Surveillance and Intelligence Commissioner, replacing the three existing Commissioners' offices.
- The controversial proposals contained in the *Draft Communications Data Bill* to provide for the compulsory retention of web logs (internet connection records) and third party data (the entire content of third party communications that pass over the network of a UK CSP) should not be pursued before a compelling operational case has been made out.[14]

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.[15] 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.[16]

---

[13] David Anderson QC, *A Question of Trust*, June 2015
[14] David Anderson, *A question of trust: report of the Investigatory Powers Review*, June 2015, see Executive summary paras 10-34
[15] Intelligence and Security Committee press release, 17 October 2013
[16] Intelligence and Security Committee press release, 9 October 2014

The Committee published its report on 12 March 2015. Although they were satisfied that the UK's intelligence 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.[17]
>
> The report also contains substantial recommendations about each of the agencies' intrusive capabilities, which the Committee considered essential to improve transparency, strengthen privacy protections, and increase oversight. Given the recent controversy surrounding GCHQ's bulk interception capability, the Committee scrutinised this aspect in particular detail.[18]

RUSI Report: Independent Surveillance Review

On 4 March 2014, the then Deputy Prime Minister, Nick Clegg, announced an Independent Surveillance Review, to be carried out by the Royal United Services Institute (RUSI). This review into surveillance technologies and the problems of control and oversight would examine surveillance practices in the UK in the context of new communications technologies. It would make recommendations for legislative and policy reform and would deliver a report after the General Election to be considered by the Government alongside the ISC review and the Anderson review.[19]

The report was published on 14 July 2015.[20] The accompanying press release summarised its recommendations:

> The Review Panel makes the case for a radical reshaping of the way that intrusive investigative techniques using the Internet and digital data are authorised that is fully compliant with the human rights framework.
>
> It recommends that requests for interception for the prevention and detection of serious crime in future be authorised by a senior judge, and that the warrants that are signed by Secretaries of State for purposes relating to national security (including counter-terrorism) should in future all be subject to judicial scrutiny, according to arrangements set out in the report.
>
> …

---

17 Intelligence and Security Committee, *Privacy and security: a modern and transparent legal framework*, HC 1075 2014/15, 12 March 2015, p2

18 Intelligence and Security Committee, press release, 12 March 2015

19 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.

20 RUSI, *A democratic licence to operate: report of the Independent Surveillance Review*, July 2015

Like other recent reviews, the ISR highlights inadequacies in law and oversight and calls for urgent new legislation in this session of Parliament to provide a new democratic mandate for digital intelligence. The present arrangements are too complex to be understood by the citizen and have contributed to a public credibility gap that must be addressed. The Review therefore sets out ten tests that any new legislation must pass before it can be regarded as giving the police and the intelligence agencies a democratic licence to operate.[21]

[21] RUSI News, *Independent Surveillance Review publishes report: 'A Democratic Licence to Operate'*, 14 July 2015

3. Part 1: General protections

What does the Bill do?

Part 1 of the Bill sets out key principles and creates a number of offences.

Clauses 2-6 define interception and "lawful authority"; create an offence of unlawful interception; and provide for the imposition of fines in situations in which unlawful interception has taken place unintentionally.

Clause 7 sets out the requirements for requesting overseas interception.

Clause 8 creates an offence of unlawfully obtaining communications data.

Clause 9 and Schedule 2 abolish existing powers to acquire communications data under various pieces of legislation. This is in order to ensure that communications data may only be acquired subject to the procedure and safeguards contained in the Bill.

Clauses 10 and 11 relate to equipment interference (hacking), setting out the conditions in which a warrant must be sought. A warrant must be sought under the Bill for equipment interference the purpose of which is to obtain communications or private information, if the conduct involved would otherwise constitute an offence under the *Computer Misuse Act 1990* and there is a connection to the British Islands.

Equipment interference
Equipment interference (also known as computer network exploitation (CNE) or cyber espionage) is the practice of gaining access to people's devices and computers in order to monitor its data, such as geolocation, texts and emails, in real time.

What did the reports say?

Anderson

The Anderson Report recommended that existing legislation should be replaced by a comprehensive new law, drafted from scratch, which affirms the privacy of communications and prohibits interference with them by public authorities, save on specific terms. The new law should replace both RIPA and existing powers under other pieces of legislation in this area.[22]

Intelligence and Security Committee

The purposes, functions, capabilities and obligations of the Agencies should be clearly set out in a new single Act of Parliament. This should be distinct from legislation covering law enforcement and other bodies currently covered by RIPA.[23] The new legislation should clearly list each intrusive capability available to the Agencies, and set out the purposes for which it can be used, the relevant human rights obligations, authorisation procedures and safeguards.

[22] Recommendations 1, 6 and 7.
[23] Annex A, paras XX & YY

The law should be amended to make abuse of intrusive capabilities (such as interception) a criminal offence.[24]

Independent Surveillance Review

Current surveillance powers are needed but they require a new legislative framework and oversight regime. Specifically, RIPA Part I, DRIPA and Part 3 of CTSA 2015 should be replaced by a comprehensive new law.[25]

[24] Annex A, para T
[25] Recommendation 1

4. Part 2: Lawful interception of communications

What does the Bill do?

Chapter 1

Clauses 12 and 13 provide for the various types of interception warrant that may be sought under the Bill. The three types of warrant are:

- A targeted interception warrant authorises the interception of communications and acquisition of associated communications data. It may relate to a particular person, organisation or premises, or groups of connected subjects.
- A targeted examination warrant authorises the examination of intercepted material obtained under a bulk interception warrant.
- A mutual assistance warrant authorises requests for, and the provision of, assistance with overseas interception.

Clauses 14-22 provide for the authorisation of warrants. The Secretary of State or Scottish Minister may issue a warrant if he or she believes that it is necessary on certain grounds and proportionate. The grounds are national security, preventing or detecting serious crime, safeguarding the economic wellbeing of the UK, or giving effect to an international mutual assistance agreement. The decision is then subject to approval by a Judicial Commissioner (see Part 8 on oversight arrangements for further detail). The Judicial Commissioner must look at the necessity and proportionality test applied by the Secretary of State or Scottish Minister on the same grounds as would be applied by a court in an application for judicial review. If the Judicial Commissioner refuses to approve a warrant they must set out written reasons for the refusal. The requesting agency may then seek to address any concerns and resubmit the request. The Secretary of State or Scottish Minister may ask the Investigatory Powers Commissioner to reconsider an application that has been refused but if the Investigatory Powers Commissioner also refuses it there is no further appeal process. In urgent cases a warrant may be issued without the approval of a Judicial Commissioner, but the Judicial Commissioner must still be notified and must decide whether to approve the warrant within five working days. If the Judicial Commissioner refuses to approve the warrant then it ceases to have effect.

Clause 16 requires the Secretary of State to consult the Prime Minister before deciding to issue a targeted interception or examination warrant where the subject is a member of either House of Parliament; the Scottish Parliament; the National Assembly for Wales; the Northern Ireland Assembly; or a UK member of the European Parliament.

Clauses 23-28 set out the information that must be contained in a warrant, the normal duration of warrants, and the process for the renewal, modification and cancellation of warrants.

The Wilson Doctrine

The convention that MPs' communications should not be intercepted by police or security services is known as the 'Wilson Doctrine'. It is named after the former Prime Minister Harold Wilson who announced the policy in 1966 in response to a number of parliamentary questions from MPs who were concerned that their phones were being tapped.

Recent case law has established that the doctrine does not have any legal effect, and that in practice the Secretary of State would consult the Prime Minister before authorising a warrant to intercept an MP's communications.

Clauses 29-31 deal with the implementation and service of warrants, and impose a duty on operators to assist with implementation. The operator must take all reasonably practicable steps to give effect to the warrant, whether or not they are located in the UK. Any requirements or restrictions under the laws of the country in which the operator is based are relevant to determining what is reasonable.

Clause 31 creates an offence of knowingly failing to comply with an interception warrant.

Chapter 2

Clauses 32-38 set out other limited forms of lawful interception. These include interception with consent; interception in prisons and psychiatric hospitals; interception for certain regulatory and enforcement purposes; and, interception for certain business purposes.

Clause 39 sets out the conditions for complying with overseas interception requests.

Chapter 3

Clauses 40 and 41 set out safeguards for the storage and disclosure of material obtained under a warrant.

Clause 42 provides that material obtained under a warrant may not be used in legal proceedings.

Clause 43 imposes a duty not to disclose the existence or details of a warrant or any intercepted material and clause 44 creates an offence of unauthorised disclosure.

What did the reports say?

Anderson

Specific interception warrants should be issued and renewed on the authority of a Judicial Commissioner.[26]

Warrants should only be granted for the purposes of:

- Preventing or detecting serious crime (including giving effect to a mutual legal assistance agreement); or
- In the interests of national security (including safeguarding the economic well-being of the UK in a respect directly linked to the interests of national security).[27]

Where a warrant is sought for the purpose of protecting national security, and the purpose relates to the defence of the UK or the Government's foreign policy, the Secretary of State should have the power to certify that the warrant is required for those purposes.[28]

Arrangements should be put in place for the consideration of urgent applications.[29]

[26] Recommendations 20 and 22
[27] Recommendation 28
[28] Recommendation 30
[29] Recommendation 31

Specific interception warrants should be limited to a single person, premises or operation. Where a warrant relates to an operation, each person or premises to which the warrant is to apply should be individually specified in a schedule to the warrant.

Extraterritorial application should continue to be asserted in relation to warrants (pending a long-term solution).[30]

Intelligence and Security Committee

The targeted interception of communications is an essential investigative capability.[31]

Ministers should continue to be responsible for issuing warrants, because they are able to take account of the wider context of warrants and are democratically accountable.[32]

Disclosure of the existence of a warrant should be permissible where the Secretary of State considers that this could be done without damage to national security.[33]

Thematic warrants should be used sparingly and authorised for a shorter timescale than a targeted warrant.[34]

Independent Surveillance Review

Where a warrant is sought for a purpose relating to the detection or prevention of serious crime, it should be authorised by a judicial commissioner, and a copy provided to the Home Secretary.

Where a warrant is sought for purposes relating to national security, the warrant should be authorised by the Secretary of State, subject to judicial review by a judicial commissioner. The review should take place before implementation of the warrant, except in urgent cases.

[30] Recommendation 25. The Government have asserted that warrants issued under Part 1 of RIPA have extra-territorial effect, that is, they may be served on CSPs overseas in the same way as they would be on a CSP in the UK. This was made explicit by section 4 of DRIPA, which amended RIPA to this effect. However, the Anderson Report states that overseas CSPs are generally unhappy with this assertion, and do not necessarily accept it. Further, engagement with overseas companies has to date been on an entirely voluntary basis (see paras 11.15-11.28)

[31] Annex A, para A

[32] Ibid, paras FF & GG

[33] Ibid, para C

[34] Ibid, para D

5. Part 3: Authorisations for obtaining communications data

What does the Bill do?

Clauses 46-47 provide for the power to grant authorisations for obtaining communications data.

Public bodies listed in Schedule 4 ("relevant public authorities") have the power to obtain communications data. These include law enforcement agencies, security and intelligence agencies, government departments, regulatory bodies and the NHS. An authorisation may be granted where a designated person (designated senior officer) at the public authority in question (also listed in Schedule 4) is content that a request is necessary and proportionate for one of 10 purposes:

- In the interests of national security;
- In the interests of preventing or detecting crime or preventing disorder;
- In the interests of the economic well-being of the UK, so far as those interests are also relevant to the interests of national security;
- In the interests of public safety;
- For the purposes of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any such injury or damage;
- To assist investigations into miscarriages of justice;
- To assist in identifying a person who has died or is unable to identify themselves because of a physical or mental condition; or
- For the purpose of exercising functions relating to the regulation of financial services and markets, or financial stability.

Public authorities can only obtain communications data for these purposes, and only certain authorities can use certain purposes (as listed in Schedule 4).

Authorisations must be given by a designated person who is independent of the operation or investigation in question, save in exceptional circumstances such as when there is an imminent threat to life. The authorisation may permit conduct for the purposes of obtaining data, including:

- Serving a notice on a telecommunications service provider that requires them to disclose the relevant data;
- Serving a notice on a telecommunications service provider that requests that they obtain and then disclose the relevant data;
- Acquiring the data directly from a communications service provider through a secure auditable system.

Clause 47 places additional restrictions on the purposes for which internet connection records (ICRs) may be obtained. ICRs may only be obtained for the following purposes:

- To identify the sender of an online communication;
- To identify which communication services a person has been using, for example determining whether they are communicating through apps on their phone;
- Identifying where a person has accessed illegal content, for example an internet service hosting child abuse imagery.

Local authorities are prohibited from acquiring ICRs for any purpose.

Clause 48 sets out the information that must be contained in an authorisation or authorisation notice, including the purpose for which it is granted and the conduct that is authorised.

Clause 49 sets a limit of one month on the duration of authorisation, and provides for renewal and cancellation.

Clause 50 places a duty on CSPs to comply with requests for communications data in so far as is reasonably practicable.

Clauses 51-53 relate to the filtering of communications data. They provide a power for the Secretary of State to establish a "Request Filter" system, whereby when a complex request for communications data is made by a public authority, any material that is not directly relevant to the investigation or operation would be filtered out before the data is supplied. Data that is not relevant will be deleted. Oversight of the Request Filter would be provided by the Investigatory Powers Commissioner, to whom would be submitted an annual report on the operation of the system, and an immediate report of any significant processing errors. Clause 67 provides that the Secretary of State's powers in these provisions may be transferred to a public authority; Schedule 5 contains further safeguards with respect to such arrangements.

Clauses 54-56 provide for the definition of "relevant public authority" and "designated senior officer" for the purposes of Part 3, as listed in Schedule 4. The Secretary of State may modify these provisions through regulations.

Clauses 57-59 provide that local authorities are relevant public authorities for the purposes of Part 3, but they may only obtain communications data through a shared single point of contact service (see below), and with the approval of a relevant judicial authority. In England and Wales this would be a justice of the peace, in Northern Ireland a district judge, and in Scotland a sheriff.

Clause 60 provides that, before granting an authorisation, the designated person must consult a single point of contact (SPoC), unless there are exceptional circumstances. A SPoC is an officer in a relevant public authority trained to facilitate lawful acquisition of communications data and effective cooperation between public authorities and CSPs. SPoCs have a responsibility to advise those

Internet connection records

An internet connection record is a record of the internet services a specific device has connected to, such as a website or instant messaging application. It does not reveal every webpage that a person has visited, or what they did on a particular webpage

applying for the acquisition of communications data and designated persons that authorise the applications.

Clause 61 provides that a public authority must obtain the approval of a Judicial Commissioner before obtaining communications data which would identify a journalist's source, unless there is an imminent threat to life. There is no requirement to notify the source or their legal representative of the application.

Clauses 62-64 provide for agreements to allow designated senior officers and SPoCs to be shared between public authorities.

Clause 65 provides that any conduct carried out in accordance with an authorisation or notice is lawful.

Clause 66 creates an offence of unlawful disclosure of any requirement imposed on a CSP or any request made in pursuance of an authorisation, in accordance with Part 3.

Clause 69 provides for the extra-territorial application of Part 3. Therefore overseas CSPs that handle communications data of UK citizens are covered by these provisions.

What did the reports say?

Anderson

Public authorities with relevant criminal enforcement powers should in principle be able to acquire communications data. There should be a mechanism for removing public authorities which no longer need the powers and for adding those which need them.[35]

Authorisations for the acquisition of communications data should be issued on the authority of a designated person authorised to do so by an authorising body.[36] Authorisations should only be given if the designated person is satisfied that it is necessary and proportionate to do so.[37]

When data is sought which relates to a person known to be a member of a profession that handles privileged or confidential information (such as doctors, lawyers, journalists, MPs or ministers of religion), the designated person should be required to ensure that special consideration is given to the possible consequences and the application should be flagged to the new oversight body.[38]

Where data is sought for the purpose of determining matters that are confidential or privileged, judicial authorisation should be sought.[39]

Judicial authorisation should also be sought for novel or contentious requests.[40]

---

[35] Recommendation 50
[36] Recommendations 20 and 23
[37] Recommendation 55
[38] Recommendation 67
[39] Recommendation 68
[40] Recommendation 70.

Extraterritorial application should continue to be asserted in relation to authorisations (pending a long term solution).[41]

Intelligence and Security Committee

Communications data do not require the same degree of protection as the full content of a communication. However, some categories of communications data have the potential to reveal details about a person's private life that are more intrusive than the basic 'who, when and where' of a communication, and therefore require greater safeguards.[42]

There should always be a clear line of separation within the Agencies between investigative teams who request approval for a particular activity, and those within the Agency who authorise it.[43]

Independent Surveillance Review

There should be a periodic review of which public bodies have the authorisation to use intrusive powers and all relevant applications from authorised public bodies to obtain communications data should be made via the National Anti-Fraud Network.[44]

[41] Recommendation 24
[42] Annex A, paras V & W
[43] Ibid, para HH
[44] Recommendation 4

6. Part 4: Retention of communications data

What does the Bill do?

Clauses 72 and 73 provide a power for the Secretary of State to require the retention of communications data and set out the matters that the Secretary of State should consider before giving a requirement notice to a CSP.

Relevant communications data is defined as that which may be used to identify:

a. The sender or recipient of a communication,

b. The type, method or pattern of a communication,

c. The type, method or pattern, or fact, of communication,

d. The telecommunications system from, to or through which, or by means of which, a communication is or may be transmitted,

e. The location of any such system, or

f. The internet protocol address, or other identifier, or any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program.

In addition to phone numbers, email addresses and source IP addresses, this includes internet connection records (for further information see Box 2 below).[45]

Clause 73 permits the recipient of a notice to refer it back to the Secretary of State if they consider an obligation unreasonable. The Secretary of State must review the notice in consultation with the Technical Advisory Board and the Investigatory Powers Tribunal, and may then vary, revoke or confirm the notice.

Clauses 74 and 75 require CSPs to take steps to ensure that retained data is stored securely, protected against unlawful disclosure, and destroyed when retention ceases to be authorised.

Clauses 76 and 77 deal with the variation, revocation and enforcement of notices.

Clause 79 provides that CSPs based overseas may comply with a retention notice but they cannot be compelled to do so.

[45] See the Government's Operational Case for the Retention of Internet Connection Records, Draft Investigatory Powers Bill: overarching documents, Gov.uk [accessed 19 November 2015]

Box 2: Retention of Internet connection records

What is an internet content record (ICR)?

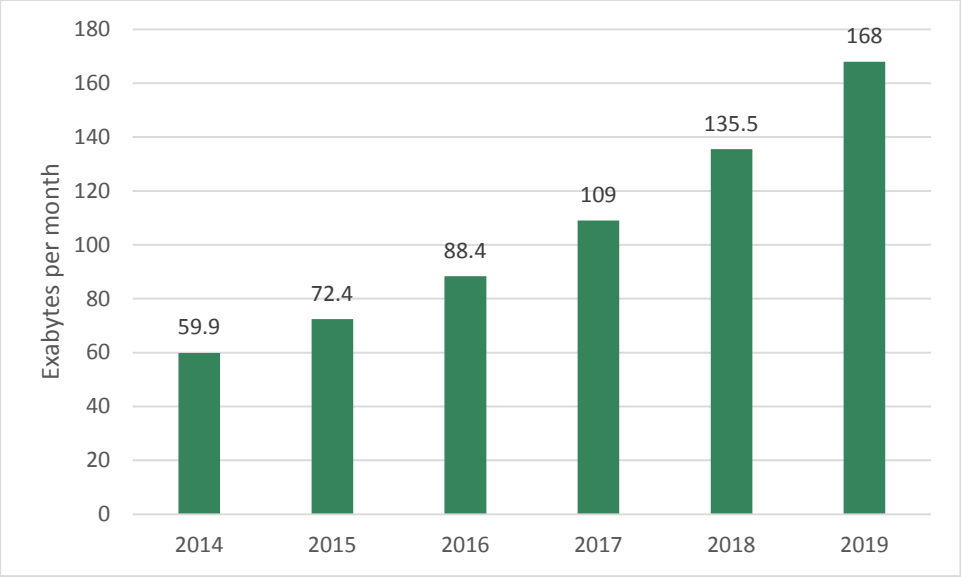
The draft Bill will create provisions for UK CSPs to retain internet content records as communications data. The Home Office define this as the 'who', 'when', 'where' and 'how' of a communication, often referred to as the 'metadata'. But it does not include the content of a communication—every web page that a person has visited or any action carried out on that web page.

Distinguishing between content and metadata is not necessarily straightforward because the web is not a single application. For a typical internet user, a number of different services are being used at any one time all of which blur the lines between content and metadata. At present, in order to understand what someone is doing online, CSPs effectively need to track all of the data all the time.

How much data will CSPs have to store?

A conservative estimate is that a tenth of all internet traffic could be considered as metadata. Cisco have forecast global internet traffic to nearly triple by 2019, up from nearly 60 exabytes per month in 2014.[46] One Exabyte is equal to 1 billion gigabytes. There are technical difficulties and concerns over the costs and of the feasibility of storing this much data both now and in the future.

Forecast Global Monthly Internet Protocol (IP) Traffic, 2014-2019



Source: Cisco VNI Global IP Traffic Forecast, 2014–2015

What did the reports say?

Anderson

The Home Secretary should be able by notice to require service providers to retain relevant communications data for periods of up to one year.[47]

Government should formulate an operational case for adding web logs (internet connection records) to the data categories that CSPs may be

[46] Cisco, *Cisco VNI Global IP Traffic Forecast, 2014–2019*, May 2015
[47] Recommendation 14

required to retain. Full consideration should be given to alternative means of achieving those purposes.

If a sufficiently compelling operational case has been made out, a rigorous assessment should then be conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained. [48]

The rules regarding retention of data should be compliant with EU law (as set out in the Digital Rights Ireland case) and the European Convention on Human Rights.[49]

Intelligence and Security Committee

It is essential that the Agencies maintain the ability to access communications data.[50]

[48] Recommendation 15
[49] Recommendation 16
[50] Annex A, para U

7. Part 5: Equipment interference

What does the Bill do?

Clauses 81-83 provide for warrants for equipment interference. There are two types of warrant:

- Targeted equipment interference warrant – authorises the interference with equipment for the purpose of obtaining communications, private information or equipment data. It may authorise the recipient to obtain, disclose, monitor and examine any such material. Any conduct necessary can be carried out in order to give effect to an equipment interference warrant, except activities which should be carried out under an interception warrant.
- Targeted examination warrant – authorises the person to whom it is addressed to carry out the examination of material obtained under a bulk equipment interference warrant.

Box 2: Equipment interference

Equipment interference (also known as Computer Network Exploitation (CNE) or cyber espionage) is the practice of gaining access to people's devices and computers in order to monitor data, such as geolocation, texts and emails, in real time.

Equipment interference is not passive. It is more likely to involve actively breaking into an adversary's computer network in order to monitor, disrupt, deny or degrade their communications. This could be as straightforward as using someone's login credentials to gain access to data held on a computer. But there are also more sophisticated means of gaining access to people's devices and computers, such as through infecting them with malware.

Equipment interference is one way in which Law Enforcement Agencies can get access to otherwise encrypted communications. The Home Office factsheet to the draft Bill explains the rationale for enabling equipment interference as follows:

> Equipment Interference is used to secure valuable intelligence to enable the Government to protect the UK from individuals engaged in terrorist attack planning, kidnapping, espionage or serious organised criminality. It also helps law enforcement agencies to protect the most vulnerable members of society.

Equipment interference is primarily used within military institutes and organisations in order to exploit, attack and defend against adversarial entities or malicious users. It consists of techniques and processes that use computers or computer networks to penetrate targeted systems and networks. For instance in November 2013, it was revealed (as part of the leaked Snowden files) that the US National Security Agency (NSA) had reportedly hacked into more than 50,000 computer networks around the world as part of its global intelligence gathering efforts.

Clauses 84-89 deal with the authorisation of equipment interference warrants. Warrants may be issued by the Secretary of State following an application by or on behalf of the heads of the intelligence services, namely GCHQ, the Security Service (MI5) and the Secret Intelligence Service. They must be necessary on the grounds of national security, preventing or detecting serious crime, or in the interests of the economic well-being of the UK, and proportionate. In the case of serious crime in Scotland, warrants must be authorised by Scottish Ministers.[51] Warrants may also be issued to the Chief of Defence Intelligence, but only for national security purposes. Decisions to sign

[51] Due to devolution arrangements.

warrants must be taken personally by the Secretary of State or Scottish Minister, and where the purpose of the application is to obtain the communications of a parliamentarian, the Prime Minister must be consulted.

Warrants may be applied for by law enforcement officers and issued by a law enforcement chief, for the purpose of preventing and detecting serious crime, subject to the same test of necessity and proportionality.

Clauses 90-92 provide that, as with interception warrants, equipment interference warrants must be approved by a Judicial Commissioner, applying the same principles as in an application for judicial review, to determine whether the decision maker has properly considered necessity and proportionality. In urgent cases, approval may be sought after the warrant has been issued.

Clause 93 sets out the information that must be included in a warrant application, such as the intended activities and reasons why the warrant is needed.

Clauses 94-98 provide for the duration, renewal, modification and cancellation of warrants.

Clauses 99 and 100 provide that the recipient of a warrant may serve a copy of it on anyone they think may be able to help, and that a warrant may be served on a person outside the UK, if it requires their assistance.

Clause 101 places a duty on telecommunications providers to assist with the implementation of equipment interference warrants.

Clause 102 creates an offence of unauthorised disclosure of the existence of such a warrant.

Clause 103 requires that safeguards be put in place to protect any data acquired and clause 104 provides that police forces may only apply for warrants where there is a connection to the UK.

What did the reports say?

Anderson

Equipment interference (referred to as CNE) should be brought into the new law and made subject to equivalent conditions as those recommended in relation to interception and the acquisition of communications data.[52]

Intelligence and Security Committee

Consideration should be given to creating a specific authorisation regime in relation to the use of IT Operations against computers or networks in order to obtain intelligence.

[52] Recommendations 6 and 21

8. Part 6: Bulk warrants

What does the Bill do?

Chapter 1: Bulk interception warrants

Clauses 106-121 deal with bulk interception warrants. Bulk interception warrants allow for the collection of a volume of communications of persons who are outside the UK, followed by the selection of specific communications to be read, looked at or listened to.

Warrants may only be sought where the main purpose is to obtain overseas related communications or related communications data for certain specified purposes, one of which must be national security.

Warrants may only be applied for by or on behalf of the heads of the intelligence services and must be issued personally by the Secretary of State, subject to the approval of a Judicial Commissioner.

Clause 108 provides that where a warrant is likely to require the cooperation of an overseas CSP, the Secretary of State must consult with the CSP before issuing the warrant, and must consider the costs and technical feasibility.

Clause 119 provides for safeguards relating to the examination of intercepted material and related communications data which has been acquired under a bulk interception warrant. Material may only be examined where necessary for the operational purposes stated in the warrant, and proportionate. Where material relates to a person known to be in the British Isles a targeted examination warrant is required, approved by a Judicial Commissioner.

Chapter 2: Bulk acquisition warrants

Clauses 122-134 relate to the acquisition of communications data in bulk.

Many of the same provisions apply as to bulk interception warrants. Bulk acquisition warrants may only be sought by the intelligence agencies for the purposes of protecting national security, and are granted by the Secretary of State, subject to approval by a Judicial Commissioner.

CSPs may be required to disclose specified communications data in their possession or to obtain and disclose data not in their possession, and warrants may be issued on a forward looking basis.

The Secretary of State is required to ensure arrangements are in place to limit the disclosure of data, and that data is held securely and destroyed when there are no longer grounds for retaining it.

Chapter 3: Bulk equipment interference warrants

Clauses 135-149 deal with bulk equipment interference. Bulk equipment interference collects data relating to a number of devices; it is not targeted against particular persons, organisations or locations, or equipment that is being used for particular activities.

Bulk equipment interference warrants are aimed at obtaining overseas related communications, private information or equipment data.

What did the reports say?

Anderson

There should be two types of bulk warrant: bulk interception warrants and bulk communication data warrants. A bulk interception warrant should never be applied for, approved or authorised when a bulk communications data warrant would suffice.[53]

Bulk interception warrants should be targeted at communications of persons believed to be outside the UK. Consideration should be given to whether an analogous restriction is necessary or desirable in relation to bulk communications data. [54]

As with intercept warrants, where the purpose relates to national security, the Secretary of State should certify that it is necessary for that purpose. Otherwise authorisation should be given by a Judicial Commissioner.[55]

Intelligence and Security Committee

Existing bulk interception is not indiscriminate, but involves a degree of targeting and filtering. It is essential that the Agencies can 'discover' unknown threats. Targeted techniques only work on known threats; bulk techniques are essential to enable the Agencies to discover threats in the first place. Existing capabilities should remain available, provided that they are tightly controlled and subject to safeguards.[56]

The Government should clarify the definition of 'external communications' –where at least one end is overseas - under RIPA in relation to internet communications, to make clear which communications are included.[57]

Searching for and examining the communications of a person known to be in the UK, or a UK national who is overseas, should require a specific warrant authorised by the Secretary of State.

The current arrangements in the *Telecommunications Act 1984* lack clarity and transparency, and should be clearly set out in law, including safeguards and statutory oversight arrangements.[58]

Independent Surveillance Review

The capability of the security and intelligence agencies to collect and analyse bulk data should be maintained with stronger safeguards as set out in the Anderson Report. Warrants should be subject to judicial authorisation.[59]

---

[53] Recommendation 42
[54] Recommendation 44
[55] Recommendations 46-48
[56] Annex A, paras F-M
[57] Ibid, para O
[58] Ibid, para VV
[59] Recommendation 8

9. Part 7: Bulk personal dataset warrants

What does the Bill do?

Clauses 150-166 provide for bulk personal dataset (BPD) warrants. A BPD is a dataset containing information about a wide range of people, most of whom are not of interest to the security and intelligence agencies. Examples provided by the Home Office include lists of people who have a passport or firearms license, or the electoral role.[60]

The intelligence services may only obtain, retain or examine a BPD with a warrant, unless the material is governed by another regime contained in the Bill.

Two types of warrant are available:

- A class warrant – authorises the intelligence services to obtain, retain or examine BPDs that fall within a class described in the warrant.
- A specific warrant – authorises the intelligence services to obtain, retain and examine a BPD described in the warrant. These warrants are relevant where the dataset concerned does not fall within a class described by an existing BPD warrant, for example where a new or novel dataset is obtained, or where the dataset may raise issues of sensitivity such that it would be appropriate for the Secretary of State to issue a specific warrant.

The Secretary of State may authorise both types of warrant if s/he believes that it is necessary and proportionate, and that satisfactory handling arrangements are in place. This is subject to approval by a Judicial Commissioner.

As with other warrants in the Bill, the decision to issue must be made personally by the Secretary of State, and a procedure is prescribed for the issue of warrants in urgent cases. The duration, renewal, modification and cancellation of BPD warrants are also provided for, consistent with the rest of the Bill.

What did the reports say?

Intelligence and Security Committee

Bulk datasets are an increasingly important investigative tool for the Agencies. In the interests of transparency, this capability should be clearly acknowledged and put on a specific statutory footing, along with provision for oversight.[61]

[60] Bulk Personal Dataset Factsheet
[61] Annex A, paras X & Y

10. Part 8: Oversight arrangements

What does the Bill do?

Chapter 1: Judicial Commissioners

Clauses 167-187 make provision for a new oversight body – the Investigatory Powers Commission (IPC). The IPC will be headed by the Investigatory Powers Commissioner and supported by Judicial Commissioners, who must have held high judicial office (together known as the Judicial Commissioners). The Judicial Commissioners are to be appointed by the Prime Minister.

The Investigatory Powers Commissioner will replace the existing Intelligence Services Commissioner, Surveillance Commissioner, and Interception of Communications Commissioner.

The IPC will report annually to the Prime Minister, and may report on other matters as it deems necessary, or as requested by the Prime Minister.

Clause 171 provides for a process whereby people can be informed of serious errors in the use of investigatory powers. A serious error would be a failure by a public authority to comply with a requirement over which the IPC has oversight which caused significant prejudice to the person concerned. In these circumstances the Investigatory Powers Tribunal (IPT) must be informed. If the IPT agrees that a serious error has occurred it must decide whether it is in the public interest for the person concerned to be informed. If the IPT decides to inform the person concerned, they must also be informed of their right to bring a claim in the IPT, and provided with the necessary information.

Public authorities and CSPs will be subject to a requirement to provide the IPC with any information, documents or assistance required to carry out oversight functions.

Chapter 2: Other arrangements

Clause 179 provides for the Secretary of State to issue Codes of Practice governing the use of powers contained in the Bill, as set out in Schedule 6. These must include provision for the protection of journalistic sources and legally privileged material.

Clause 180 provides for a right of appeal from the IPT to the Court of Appeal on a point of law.

Clauses 181-183 provide for oversight and advisory functions in relation to the retention of communications data under Part 4 of the Bill, including the retention of a Technical Advisory Board.

What did the reports say?

Anderson

The Interception of Communications Commissioner's Office, the Office of the Surveillance Commissioners and the Intelligence Services

Commissioner should be replaced by a new Independent Surveillance and Intelligence Commission (ISIC).[62]

ISIC, through its Judicial Commissioners, should have the power to issue, renew and modify warrants. Judicial Commissioners should hold or have held high judicial office.[63]

The existing audit and inspections functions of the current Commissioners should be transferred to ISIC.[64]

ISIC should have the power to inform a subject of an error on the part of a public authority or CSP, and of the right to lodge a complaint with the IPT.[65]

The jurisdiction of the IPT should be expanded to cover circumstances where it is a CSP rather than a public authority which was at fault.[66]

There should be a right of appeal to an appropriate court from rulings of the IPT on points of law.[67]

The IPT should have the same power as the High Court to make a declaration of incompatibility under section 4 of the *Human Rights Act 1998*.[68]

Intelligence and Security Committee

The Commissioners should have increased oversight responsibilities, and all their functions should be put on a statutory footing.[69]

While oversight systems in other countries include an Inspector General function, this is often more of an internal audit function. It is important to maintain the external audit function that the existing Commissioners provide. [70]

There should be a domestic right of appeal from the IPT.[71]

Sensitive professions should not have automatic immunity from interception, but some professions may justify heightened protections, provided for in statute.[72]

Independent Surveillance Review

The existing Commissioners should be replaced by a new single body: a National Intelligence and Surveillance Office with four main areas of responsibility: inspection and audit; intelligence oversight; legal advice; and public engagement.

---

[62] Recommendation 82
[63] Recommendations 84 & 85
[64] Recommendation 89
[65] Recommendation 99
[66] Recommendation 113
[67] Recommendation 114
[68] Recommendation 115
[69] Annex A. para II & JJ
[70] Ibid, para KK
[71] Ibid, para LL
[72] Ibid, para UU

The Technical Advisory Board should be replaced with an Advisory Council for Digital Technology and Engineering, which would be a statutory non-departmental public body. The Council should keep under review the domestic and international situation with respect to the evolution of the internet, digital technology and infrastructure. It should also provide advice to ministers and departments and manage complaints from CSPs on notices they consider unreasonable.

The IPT should find ways to be less opaque and should hold open hearings except where closed proceedings are necessary in the public interest.[73]

The IPT should have the ability to test secret evidence and there should be a domestic right of appeal.[74]

The judicial commissioners should be able to refer cases to the IPT where they find a material error, arguable illegality or disproportionate conduct.[75]

[73] Recommendations 11 & 12
[74] Recommendations 13 & 14
[75] Recommendation 16

11. Part 9: Miscellaneous and general provisions

What does the Bill do?

Chapter 1: Miscellaneous

Clause 184 introduces Schedule 7, which makes provision for the combination of targeted interception warrants or targeted interference warrants with other warrants or authorisations.

Clause 185 provides that CSPs must receive a contribution towards their compliance costs and clause 186 enables the Secretary of State to put measures in place to facilitate compliance.

Clause 187 would amend the *Intelligence Services Act 1994* in relation to certain functions of GCHQ.

Clause 188 provides that the Secretary of State may issue a "national security notice" requiring a CSP to take steps in the interests of national security. National security notices may only require conduct that the Secretary of State considers to be proportionate, for example the provision of services or facilities to assist an intelligence service to carry out its functions more effectively. A notice must not be used to require the taking of steps for which a warrant or authorisation would otherwise be required under the Act.

Clause 189 provides that the Secretary of State can use regulations to impose obligations on CSPs, via "technical capability notices", to facilitate assistance in relation to authorisations under Parts 2, 3, 5 and 6 of the Bill. Obligations may include obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data, and obligations relating to the security of any postal or telecommunications services. Before making regulations under this clause the Secretary of State is obliged to consult the Technical Advisory Board and CSPs.

Clauses 190 and 191 make further provision in relation to "national security notices" and "technical capability notices", including the matters that the Secretary of State should take into account before issuing a notice; the duty to comply; and the process for review of a notice.

Clause 192 amends the *Wireless Telegraphy Act 2006* to avoid duplication with the Bill in relation to interception powers.

Chapter 2: General

The remaining clauses provide for definitions, procedures to be used for making regulations, financial provision and other technical matters.

12. Reaction

Political

The initial political reaction to the Home Secretary's statement introducing the Bill was generally positive. Shadow Home Secretary Andy Burnham said:

> From what the Home Secretary has said today, it is clear to me that she and the Government have listened carefully to the concerns that were expressed about the draft Bill that was presented in the last Parliament. She has brought forward much stronger safeguards, particularly in the crucial area of judicial authorisation. It would help the future conduct of this important public debate if the House sent out the unified message today that this is neither a snooper's charter, nor a plan for mass surveillance.[76]

Nick Clegg said:

> The current Bill is a much improved model [compared to the Draft Communications Data Bill], although I have the feeling that, under the bonnet, it retains some of the flaws of its predecessor. The Home Office has clearly put in a lot of work, which I welcome, as I do the dropping of some of the key provisions on third-party data and encryption.[77]

Joanna Cherry, Home Affairs spokesperson for the SNP, said:

> I thank the Home Secretary for her statement, its tone and the care taken to address many of the concerns raised.
>
> …
>
> We have our political differences, and I am sure there will be some over the content of the draft Bill … but I think we all agree that we have a responsibility to protect the rights of our fellow citizens while being realistic about the threats we face.[78]

Writing in the Guardian on 5 November, Shadow Home Office Minister Keir Starmer welcomed the introduction of judicial authorisation for warrants, suggesting that it would help to restore trust in the system. However, he also suggested that it would be important to ensure that there would be real judicial scrutiny, and not a rubber stamping exercise.[79]

Andy Burnham subsequently wrote to the Home Secretary expressing reservations about aspects of the Bill:

> I have now had the opportunity to study your proposal in detail and have taken advice from the Shadow Justice Secretary. This has given rise to concerns that the safeguards you are proposing are not as strong as it appeared when they were presented to the Commons.

---

[76] HC Deb 4 November 2015, c972
[77] Ibid c976
[78] Ibid c978
[79] Theresa May's investigatory powers bill is a step in the right direction, *The Guardian*, 5 November 2015

> First, on judicial authorisation, you said in your statement that the authorisation of intercept warrants would be two-stage process, or a 'double-lock'. This created the impression that both the Home Secretary and a senior judge would review the evidence. …
>
> On closer inspection of the wording of the Bill, it would seem, that it does not deliver the strong safeguard that you appeared to be accepting. …
>
> Legal advice we have sought confirms that the current working does not deliver what was believed was being proposed in terms of the Home Secretary and Judicial Commissioner double-lock for warrant authorisation.
>
> … If our understanding is correct, then I wanted to give you notice that we will be looking to amend the working of the Bill in Committee to ensure it delivers what we thought was being offered.[80]

He further suggested that the Bill needed to contain a clearly defined threshold for access to internet connection records, based on the seriousness of the crime being investigated.

David Davis has also expressed concern about the fact that the procedure for judicial authorisation of warrants only permits refusal of warrants on judicial review principles, as well as the requirement that CSPs hold communications data for up to a year.[81] Writing in the Financial Times, Mr Davis described the Bill as a missed opportunity:

> [T]he draft bill, while moving fractionally in the right direction, has serious flaws. The government has tried to bring its multitudinous powers together in a single bill. In this it has failed, with a number of important powers still lying outside the scope of the checks and oversights proposed under the draft legislation.
>
> The supposed strength of the new legislation is its "double lock" authorisation process, with both ministerial and judicial approval required for the grant of any warrant. However, the decision to retain the home secretary's authorisation process for domestic interception — the first lock of the double lock — is utterly irrational. Domestic interception should not be a political decision. In any event, this system does not offer any accountability, as ministers never answer questions on security and certainly never admit to security errors.
>
> Even with surveillance powers other than domestic interception, the proposed "double lock" falls far short of what is needed, and fails to live up to government promises. Limiting judicial commissioners to considering warrants on judicial review principles means they can overrule a home secretary only if he or she is deemed to have acted utterly unreasonably. The government has hamstrung the process, in essence turning it into a judicial rubber stamp.
>
> …
>
> The government's approach to encryption also leaves much to be desired. At least it did not go ahead with Prime Minister David

[80] Published in Labour demands stronger safeguards in Investigatory Powers Bill, New Statesman, 8 November 2015

[81] Interview, *The Guardian*, 8 November 2015

> Cameron's unwise proposal this year to ban end-to-end encryption — the unbreakable code that makes it impossible to read our online messages and transactions even if they are intercepted. Such a move would have had devastating consequences for all financial transactions and online commerce, not to mention the security of all personal data. Its consequences for the City do not bear thinking about.
>
> Instead, government policy is likely to strangle UK tech businesses, by prohibiting the spread of encryption to those services that do not already use it. This will put our communications companies at a severe disadvantage, as their overseas competitors are permitted to offer fully secure services forbidden to UK companies.
>
> The government has also retained the power to demand data from overseas service providers. However, companies will be permitted to refuse to hand over customers' data where doing so would place them in breach of laws in the country where they are based.
>
> The consequences have not been thought through. Under this regime, tech start-ups will prefer Iceland or Switzerland or Germany, where users' data will be protected from our government's demands by local regulations.

David Anderson QC

Following publication of the Bill, David Anderson published a statement on his website:

> The best thing about the Bill is that it puts Parliament in charge. For the first time, we have a Bill that sets out, for public and political debate, the totality of the investigatory powers used or aspired to by police and intelligence agencies. …
>
> Not everyone will be happy about those powers. It will now be for Parliament to decide whether they are justified. That is the way things should be in a democracy – but rarely are at the moment, anywhere in the world. Whatever the content of the eventual UK law, it will no longer be possible to describe it as opaque, incomprehensible or misleading.
>
> …
>
> The Bill also contains safeguards. My report, and that of RUSI, were particularly influential here. There will be a powerful, outward-facing super-regulator, and save in urgent cases, no warrant will enter into force without judicial approval – a reversal of consistent practice since at least the 17th century.
>
> Opinions will differ as to whether these safeguards go far enough. The judges need to be well-supported, and exposed to a sufficiently wide range of opinion for there to be no question of them operating as rubber stamps.
>
> It also needs to be asked whether there is sufficient independence in procedures for access to communications data, bearing in mind in particular the Digital Rights Ireland judgment on whose meaning the European Court of Justice has recently been asked to pronounce, and the particularly sensitive or intrusive nature of

> some data (for example, the fact that a lawyer may have communicated with a potential witness).[82]

He also made a number of media appearances, but said that he would not comment further on the draft Bill unless asked to do so by parliamentary committees.

Press

An editorial in the *Financial Times* suggested that the Bill "goes a long way towards allaying public concern about data privacy –but not far enough" and that it was "close to striking the right balance". The FT agreed with the need for strong surveillance powers, and with the introduction of judicial oversight to increase public confidence. However, the proposal to allow the security services to track citizens' use of the web "raises concern".[83]

The *Times* also felt that on the whole the Bill had struck the right balance, but emphasised the importance of parliamentary scrutiny, particularly in respect of safeguards.[84]

The *Telegraph* suggested that "There is much in the [Bill] that seeks to achieve an equilibrium between the needs of security and the requirements of privacy", also praising the Home Secretary's decision to introduce it as a draft for consultation.[85]

By contrast, the *Independent* described the proposals to retain internet connection records as "surely staggering", and questioned the analogy, offered by the Government, with an itemised phone bill.[86]

Writing in the *Guardian*, Joshua Rozenberg suggested that it is wrong to refer to the Judicial Commissioners as judges:

> They will not be sitting in court or hearing arguments from both sides. They will need to be retrained.
>
> Although the draft bill includes a person "who holds or has held high judicial office", nobody expects the post to go to anyone who is still sitting as a full-time judge.[87]

Industry

The Chief Executive of Apple, Tim Cook, is reported to have expressed concern about the legal obligation on companies to assist in operations to bypass encryption:

> Any backdoor is a backdoor for everyone. Everybody wants to crack down on terrorists. Everybody wants to be secure. The

[82] Putting Parliament in Charge, 4 November 2015, terrorismlegislationreviewer.independent.gov.uk
[83] One power too many for Britain's security state, *Financial Times*, 4 November 2015
[84] Power to Probe, *The Times*, 5 November 2015
[85] Theresa May must balance privacy and security, *The Telegraph*, 5 November 2015
[86] 'Snooper's Charter': Forcing internet providers to keep our browsing history leaves us open to security breaches, *Independent*, 4 November 2015
[87] These internet surveillance powers risk undermining the judiciary, *The Guardian*, 4 November 2015

> question is how. Opening a backdoor can have very dire consequences.[88]

Box 4: Encryption

Encryption is the process of converting information ('plaintext') into an encrypted form ('ciphertext'), which cannot easily be understood by anyone except parties authorised to 'decrypt' the information. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over an unsecured network, such as the internet.

Encryption is routinely used by Communications Service Providers (CSPs) and applications to protect data in transit sent from all sorts of devices and across all sorts of networks, not just the internet, and this can include ATM transactions, online purchases and more.

Data is encrypted using an encryption algorithm and an encryption key. Encryption algorithms are divided into two main categories: symmetric and asymmetric:

- Symmetric encryption uses the same 'key' for both encrypting and decrypting data. In symmetric encryption both sides—the encrypter, and the decrypter—need access to the same key. Thus the sender of data must exchange the key used to encrypt the data with the recipient before it can be decrypted.
- Asymmetric encryption (also known as public-key cryptography) takes readable data and encrypts it using a public key. It then decrypts it using a private (secret) key. The private key must be kept private much like the key for symmetric encryption. This enables communication without the need for sharing secret encryption keys.

Most cryptographic processes use a symmetric algorithm to efficiently encrypt data, but use an asymmetric algorithm to exchange the secret key.

End-to-end encryption

Encrypted communications are only as secure as the cryptographic keys used to decrypt the messages, which tend to be held by the communications company. There are concerns that communications companies may be forced to reveal these keys so as to monitor the otherwise encrypted communications. This is just one reason why companies have begun to offer end-to-end encryption.

End-to-end encryption is a method of secure communication where the only people who can read the messages are the people communicating. Unlike more traditional means of encryption, in end-to-end encryption the only people who have access to the cryptographic key are the two people communicating. This means that third-parties cannot access data while it's transferred from one end system or device to another—not even a company that runs the messaging service. However, there are concerns in the cybersecurity community that if CSPs are asked to provide security services with 'backdoors' to these programmes, the security of the protocol more generally will be compromised.

Giving evidence to the Science and Technology Committee, industry representative expressed concern about various aspects of the Bill, including the volume of data required to be retained and the cost of keeping it secure. It was suggested that these costs would ultimately be passed on to customers.

John Shaw, representing Sophos, also expressed concerns as to what constitutes a service provider:

> In the Bill itself there are definitions of telecom service, service providers and service operators that attempt to be very broad so as to be future-proofed, but are therefore very broad in the sense that you can define almost any form of software or communication these days as being a telecom service. I have concerns over exactly how far the powers will go. They could be interpreted as going a lot further than I believe is the intention.[89]

Another area of concern was the differential treatment of UK and non-UK-based CSPs, and specifically the risk that UK-based CSPs might be

---

[88] Interview, *The Telegraph*, 10 November 2015

[89] Oral evidence: Investigatory Powers Tribunal: technology issues, HC 573 Science and Technology Committee, 10 November 2015

placed at a competitive disadvantage by the requirement to store communications data, because it might deter non-UK citizens from trading with them. This in turn might have an impact on investment in software and hardware companies in the UK.

Civil liberties campaigns

Open Rights Group (ORG) have published an initial response to the Bill, highlighting areas of concern:

> **Legitimising bulk interception and previously unknown access to UK communications data**
>
> The draft bill spells out the powers that the security services have to collect content and data in bulk. Although this had been done for years, no one really understood the extent of GCHQ's capabilities until the Snowden leaks. The government acknowledged today that secret agencies have been going even further, accessing data in bulk from UK internet providers not just from international cables. The bill effectively endorses these previously secret –and at face value disproportionate – mass surveillance powers. This is in addition to powers to obtain bulk datasets, such as phone books, driving licenses, travel or banking records.
>
> **Retaining even more data**
>
> One of the most controversial parts of this new Bill is that ISPs will be forced to keep much more detailed data about our internet activities, such as websites we visits or apps we use in our phone. To access this data, the police would need to get a court order – this seems to be a concession to the European Court of Justice ruling last April that said there must be safeguards for accessing retained data. In July, the High Court said that parts of the Data Retention and Investigatory Powers Bill were unlawful for the same reason.
>
> We will be asking why the UK police feel they need these powers.
>
> …
>
> **Who signs off warrants?**
>
> The new Bill proposes a new system of "double-lock" where some warrants will be signed both by the Secretary of State or an authorised person, and additionally by a special judge. At face value this might seem an improvement on the current situation where judges do not have a role, but there are concerns that in practice this may simply amount to a rubber-stamp. Judges would have a very narrow role, only being allowed to check that there are grounds for the minister's decision and that procedures have been followed, but not to challenge the substance of the decision. Fully independent judicial authorisation would be a better guarantee of due process. Disappointingly, the draft new bill still allows police, councils and other agencies to obtain communications data without the need to involve a judge.
>
> **Has encryption been banned?**
>
> We don't think there was ever going to be a serious attempt to ban encryption. The Bill ask for powers to compel communications providers to assist with demands

> for interception. How companies do this will presumably be at their discretion. In some cases this might involve compromising their software to make the encryption less effective. This is something that we are sure companies will be looking into.
>
> **New hacking powers**
>
> The bill clarifies the powers of security agencies to break into our laptops and mobile phones, including worrying new powers for non-targeted mass hacking. The bill also forces internet companies to help in hacking their customers. What are the positives? We asked for a transparent law and on first reading it does seem to be very clear about the powers being given to the State. Transparency over these activities is very welcome, as it enables debate and challenges to specifics, including in the courts. There also seems to be improvements to redress, including the right to appeal rulings by the Investigatory Powers Tribunal, which is something ORG has campaigned for. The new Investigatory Powers Commissioner may also bring improvements to democratic oversight.[90]

Privacy International also questioned whether the proposal for judicial oversight of warrants represents a significant departure from the current practice of ministerial approval, and raised particular concerns about hacking and bulk interception powers.[91]

Liberty issued a press release outlining what they perceived to be the most contentious aspects of the Bill:

- The Bill does not provide for substantive judicial approval of warrants, but rather proposes a highly limited review which will in practice be a rubber stamping exercise.
- The power for the blanket retention of internet connection records is highly intrusive and unprecedented in comparable countries.
- The proposed hacking powers have the potential to do unlimited damage to the security of devices and networks and make people vulnerable to abuse.
- The Bill places the mass surveillance powers revealed by Edward Snowden on a statutory footing, rather than creating a more targeted and effective system.[92]

This response is consistent with Liberty's previously expressed opposition to bulk interception, support for judicial, as opposed to ministerial, approval of warrants, and the need for stringent safeguards to govern hacking powers.[93]

Justice have questioned the Government's claim that the Bill is comprehensive and comprehensible, pointing out that it does not

---

[90] First take on the Investigatory Powers Bill, 5 November 2015, openrightsgroup.org [accessed 18 November 2015]
[91] From Britain, with Bulk Love: A Dark Digital Magna Carta, 11 November 2015, privacyinternational.org
[92] Press Release, Liberty, 4 November 2015
[93] Liberty's Briefing on *'A Question of Trust: The Report of the Investigatory Powers Review'*, June 2015

replace RIPA in its entirety, which will still govern other forms of surveillance. Justice welcome the introduction of additional safeguards, but caution that safeguards cannot automatically render surveillance powers proportionate, necessary and lawful.[94]

Legal commentary

David Allen Green,[95] writing on the *FT* blog, has suggested that the Government must show that the judicial element of authorisation is not a "constitutional figleaf" by demonstrating how in practice the Judicial Commissioners will check, as opposed to endorse, the Secretary of State's warrant decisions. However he concludes that the real challenge is whether the measures are practical and commercial: whether the Bill will work in practice, given developments in technology; and whether overseas service providers will cooperate.[96]

Lord Pannick QC, writing in the Times, suggested that criticisms of the judicial oversight scheme are unjustified, and that it adopts "the right balance in this difficult area":

> The home secretary rightly recognised that judicial involvement in these decisions is necessary to promote public confidence in a sensitive area. It will also improve standards because the security services will not want to have their applications rejected. Judicial power is necessary to ensure that intrusive surveillance measures satisfy European human rights law and EU law. And, most fundamentally, without the judicial element, such a bill is unlikely to be approved by parliament.
>
> Andy Burnham and David Davis, the Conservative backbencher with a strong record on civil liberties issues, say that a judicial review test gives judges too little power because it only relates to "process". But it is well established that judicial review is a flexible concept, the rigour of which depends on the context. The Court of Appeal so stated in 2008 in the T-Mobile case.
>
> The closest analogy to the provisions in the draft bill is judicial review of control orders and Tpims (terrorist prevention and investigation measures). The Court of Appeal stated in the MB case in 2006 that judges applying a judicial review test must themselves consider the merits and decide whether the measure is indeed necessary and proportionate. It is true that the context there involves restrictions that vitally affect liberty — in the sense of freedom of movement. But I would expect the courts to apply a very similar approach in the present context, concerned as it is with the important issue of privacy. So those who are concerned that a judicial review test does not give judges sufficient control should be reassured.
>
> However, in a national security context, the judiciary adopts a self-denying ordinance, applying the principle stated by Lord Neuberger (president of the Supreme Court) and Lord Dyson (master of the rolls) in a Supreme Court judgment in July in the Beghal case. In a terrorism context, judges have a function that involves a "tension" between "vigilance" to ensure that the

[94] *The Draft Investigatory Powers Bill: Building a Surveillance Framework for a Digital Age?*, 6 November 2015, justice.org.uk [accessed 18 November 2015]
[95] Head of Media at Preiskel & Co and editor of Jack of Kent legal blog.
[96] *The Investigatory Powers Bill: will it work in practice?* 5 November 2015, blogs.ft.com

> powers are exercised only where necessary and proportionate, and "circumspection", because of the superior knowledge and experience of the executive in assessing risks to national security. Judges also recognise the institutional responsibility of the home secretary who is answerable to parliament. Judges therefore accord the executive a margin of discretion.
>
> That tension, and margin of discretion, is inherent in judicial control of the exercise of powers relating to national security. It would apply even if the legislation were to adopt criteria other than those applied on a judicial review application. The margin of discretion does not alter the power and duty of the judges to scrutinise decisions intensely and to impose restraints where appropriate, depending, of course, on the circumstances of the individual case.[97]

However, he also suggested that the Bill could be improved by provision for Judicial Commissioners to hear representations by lawyers acting for the person who is to be the subject of the intrusive measures.

Graham Smith, editor of the Cyberleagle blog, has written about the issue of secret interpretations of the law in the context of encryption. Citing examples from RIPA of controversial Government interpretations of the law, which would have been unlikely to come to light if not for the Snowden leaks, he suggests that a similar issue might arise if the Bill becomes law. Clause 189(4)(c) provides for the possibility that CSPs may be required to remove electronic protection (de-encrypt) material in order to assist in the implementation of a warrant. On the face of it, this does not affect end-to-end encryption where the protection is applied by the service user rather than the service provider. However, Mr Smith suggests that this provision could be subject to similarly controversial interpretation by the Home Office, and that the public would be in no position to know. As a way round this, Mr Smith suggests that the new IPC could proactively seek out and bring to public attention material legal interpretations on the basis of which powers are exercised or asserted. CSPs might also be able to bring a legal interpretation asserted against them to the attention of the oversight body.[98]

---

[97] David Pannick, Safeguards provide a fair balance on surveillance powers, *The Times*, 12 November 2015

[98] From Oversight to Insight: Hidden Surveillance Law Interpretations, 9 November 2015, cyberleagle.blogspot.co.uk

13. Further reading

Draft Investigatory Powers Bill: overarching documents, Gov.uk –

A Question of Trust: Report of the Investigatory Powers Review, terrorismlegislationreviewer.independent.gov.uk

Privacy and Security: A modern and transparent legal framework, isc.independent.gov.uk

A Democratic Licence to Operate: Report of the Independent Surveillance Review, rusi.org

Debate: Reports into Investigatory Powers, HC Deb 25 June 2015, c1081-1143

Report of the Joint Committee on the Draft Communications Data Bill, December 2012

Investigatory Powers Bill: Technology issues inquiry – oral evidence, Science and Technology Committee

BRIEFING PAPER
Number 7371, 17 November 2015

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publically available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcinfo@parliament.uk.

Disclaimer