House of Commons

Science and Technology Committee

Investigatory Powers Bill: technology issues

Third Report of Session 2015–16

HC 573

House of Commons

Science and Technology Committee

Investigatory Powers Bill: technology issues

Third Report of Session 2015–16

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed
19 January 2016

HC 573
Published on 1 February 2016
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Nicola Blackwood MP (*Conservative, Oxford West and Abingdon*) (Chair)

Victoria Borwick MP (*Conservative, Kensington*)

Stella Creasy MP (*Labour, Co-op, Walthamstow*)

Jim Dowd MP (*Labour, Lewisham West and Penge*)

Chris Green MP (*Conservative, Bolton West*)

Dr Tania Mathias MP (*Conservative, Twickenham*)

Carol Monaghan MP (*Scottish National Party, Glasgow North West*)

Graham Stringer MP (*Labour, Blackley and Broughton*)

Derek Thomas MP (*Conservative, St Ives*)

Valerie Vaz MP (*Labour, Walsall South*)

Matt Warman MP (*Conservative, Boston and Skegness*)

The following were also members of the committee during the parliament:

Liz McInnes MP (*Labour, Heywood and Middleton*)

Daniel Zeichner MP (*Labour, Cambridge*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/science and by The Stationery Office by Order of the House.

Evidence relating to this report is published on the relevant inquiry page of the Committee's website.

Committee staff

The current staff of the Committee are: Simon Fiander (Clerk), Marsha David (Second Clerk), Dr Grahame Danby (Science Clerk), Dr Elizabeth Rough (Committee Specialist), Darren Hackett (Senior Committee Assistant), Julie Storey (Committee Assistant), and Nick Davies (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 2793; the Committee's email address is scitechcom@parliament.uk.

Contents

Summary

The draft Investigatory Powers Bill was published by the Government on 4 November 2015. Ministers have been clear that the intention of this Bill is to consolidate and clarify existing legislation on the interception of communications and the acquisition of communications data and to modernise the law in the light of developments in communications technologies, in order to maintain the operational capabilities of law enforcement agencies and the intelligence and security services.

Previous attempts to legislate in this area have met with criticisms over the lack of consultation with communications service providers (CSPs) on matters of technical feasibility and cost. In our inquiry we have focused on technological aspects of the draft Bill in order to identify the main technological issues involved and how these might affect the communications businesses that will have to collect data and cooperate with the security authorities.

We have not addressed the need or otherwise for the communications monitoring provisions or whether they are proportionate to the threats they are intended to deal with. We anticipate that these matters will be covered by the Joint Committee established to scrutinise the draft Bill as a whole.

Following the failure of previous attempts to introduce data legislation, the Government has made efforts to consult and engage with communications service providers likely to be most affected by the draft Bill. However, there remain widespread doubts over the definition, not to mention the definability, of a number of the terms used in the draft Bill. This has given rise to uncertainties over the likely scope and costs associated with implementing the proposed measures. Such uncertainty is unhelpful to businesses trying to compete in a global communications market and risks undermining our strongly performing Tech sector. The fast paced nature of technological development including the growing 'internet of things' and questions around encryption developments further limits the possibility of creating legislation that can keep up with these innovations. While we well understand the security challenges of communications data, we strongly believe UK businesses must not be placed at a commercial disadvantage by measures to tackle security risks and that the full costs of implementing the additional measures in the draft Bill should be met by Government. Given that the cost of being able to do this is directly related to any future changes or developments in technology, we recognise this makes predicting accurately the cost of these measures difficult. This therefore raises concerns over any assessment of the costs of this scheme, which could increase or decrease, and so the value for money of this proposed legislation.

The Government claims that the only substantially new requirements provided for in the draft Bill relate to the retention of so-called 'internet connection records' (ICRs). By implication, other high-profile powers relating to the 'removal of electronic protection' and 'equipment interference' are already in place. However, the nature of ICRs and the true extent of the Bill's 'removal of electronic protection' and 'equipment interference' powers are precisely the subject of uncertainty and concern from business due to lack of clarity in the Bill and in the consultation so far. It is clear that greater reassurance is needed—both on the face of the Bill and in forthcoming Codes of Practice—that

businesses will not be subject to disproportionate additional burdens that will not be fully paid for.

Detailed Codes of Practice will be needed to provide a more effective means of assisting compliance, and retaining business confidence in the feasibility of investigatory powers provisions, by making their regular updating an explicit requirement in the Bill when it is introduced. The Bill should also require that at regular set intervals the Technical Advisory Board is consulted about keeping the Codes of Practice up to date—a new role we propose for that body—and allowing both the Government and business representatives to bring forward amendments. Those Codes of Practice should clearly address the requirements for protecting ICR data that will have to be retained and managed by CSPs, along with the security standards that will have to be applied to keep them safe. It is essential that the timetable for producing draft Codes of Practice must not be allowed to slip; they should be produced and debated alongside the Bill due to their particular significance for ensuring that this legislation meets its security goals and represents value for money to the taxpayer while protecting our economic priorities.

Greater flexibility and inclusiveness will be needed in respect of the operation and makeup of the Technical Advisory Board to ensure that the draft Bill's measures—if enacted—remain fit for purpose and technically feasible and subject to robust challenge. The Government should review the composition of the Board to ensure that it will have members from industry who will be able to give proper consideration, not just to the technical aspects of appeals submitted to it from CSPs concerned about ICRs or other matters, but also any concerns raised about costs. The Government should also develop a framework protocol for such mediations including any formal resolution process should disagreements regarding costs or technology persist. The Government should add to the remit of the Technical Advisory Board a role in keeping under review the domestic and international implications of the evolution of the internet, digital technology and infrastructure.

Some sectors of the communications industry have concerns that 'equipment interference' could jeopardise their business model, for example those producing and distributing open source data. Their clients may not be aware of when equipment interference happens because disclosure is not permitted. The Government should, as far as security considerations allow, produce regular information which gives the public an indication of the extent to which such measures are used and how any disagreements on this issue are resolved. This should be a core task of the new Investigatory Powers Commissioner.

If law enforcement agencies and the intelligence and security services are effectively to combat terrorism and serious crime, they must have the means to keep pace with developments in communications. They will doubtless need to continue to deploy a range of methods for intercepting and acquiring information about communications. The evidence we have received suggests there are still many unanswered questions about how this legislation will work in the fast moving world of technological innovation. There are good grounds to believe that without further refinement, there could be many unintended consequences for commerce arising from the current lack of clarity of the terms and scope of the legislation. It is essential that the integrity and security of legitimate online transactions is maintained if we are to trust in, and benefit from, the opportunities of an increasingly digital economy.

1 Introduction

1. The draft Investigatory Powers Bill was published by the Government on 4 November 2015. Ministers have been clear that the intention of this Bill is to consolidate and clarify existing legislation on the interception of communications and the acquisition of communications data. It also represents an attempt to modernise the law in the light of developments in communications technologies, to maintain the operational capabilities of law enforcement agencies and the intelligence and security services.

2. The Regulation of Investigatory Powers Act 2000 (RIPA) set out the conditions that the security services and other agencies must satisfy in order to access 'communications data' (namely information about communications but not the content of those communications). The Act also specifies what data can be accessed, by whom and for what purposes. In 2012, a draft Communications Bill (dubbed the "snoopers' charter" by its detractors) was introduced to secure further access to communications data. However, although the Joint Committee on the draft Bill saw a case for "some further access to communications data", it concluded that the draft Bill was "too sweeping", and "went further than it need or should".[1] The Bill was disproportionate, giving the Secretary of State "sweeping powers to issue secret notices to communications service providers (CSPs) requiring them to retain and disclose potentially limitless categories of data".[2] The draft Bill was also considered by the Joint Committee on Human Rights and the Intelligence and Security Committee. It was not taken forward in the last Parliament.

3. The Data Retention and Investigatory Powers Act 2014 was enacted to allow for the ongoing retention of communications data, in response to the Court of Justice of the European Union having declared the pre-existing regime under the Data Retention Directive invalid on privacy grounds. Part 3 of the Counter-Terrorism and Security Act 2015 subsequently amended the Data Retention and Investigatory Powers Act 2014 to enable the Secretary of State to require internet service providers to retain data allowing the authorities to identify the person or device using a particular IP (internet protocol) address at any given time.[3]

4. The 2015 Queen's Speech included an undertaking that "new legislation will modernise the law on communications data".[4] The Government stated that its purpose would be to:

- address ongoing capability gaps that are severely degrading the ability of law enforcement and intelligence agencies ability to combat terrorism and other serious crime;
- maintain the ability of our intelligence agencies and law enforcement to target the online communications of terrorists, paedophiles and other serious criminals;

1 Joint Committee on the Draft Communications Data Bill, Report of Session 2012-13, Draft Communications Data Bill, HL Paper 79, HC 479
2 Joint Committee on the Draft Communications Data Bill, Report of Session 2012-13, Draft Communications Data Bill, HL Paper 79, HC 479.
3 House of Commons Library Briefing Paper 7371, Draft Investigatory Powers Bill, 19 November 2015
4 https://www.gov.uk/government/speeches/queens-speech-2015

- modernise our law in these areas and ensure it is fit for purpose;
- provide for appropriate oversight and safeguard arrangements.[5]

In June 2015, the Home Secretary set out a timetable for the new legislation, publishing a draft Bill "in the autumn for pre-legislative scrutiny by a Joint Committee of Parliament, with the intention of introducing a Bill early in the new year".[6] She highlighted that because of the sunset clause in the Data Retention and Investigatory Powers Act 2014, "the new legislation will need to be in place by the end of December 2016".[7]

5. The Government also committed to ensuring that the Bill would respond to issues raised by David Anderson QC—the Independent Reviewer of Terrorism Legislation—in his report on the operation and regulation of investigatory powers.[8] David Anderson's report covered the interception of communications and communications data, the challenges posed by changing technology, new capabilities for encryption, anti-surveillance tools and the 'dark net'. During a debate on the Anderson Report in June 2015, the Home Secretary said that the Government "would accept all the principles that [the Joint] Committee set out [in 2012], including that the original draft Communications Data Bill, which was an attempt to future-proof our legislation, was too wide ranging".[9]

6. According to the Government, the draft Investigatory Powers Bill will do three things:

- First, it will bring together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will make these powers—and the safeguards that apply to them—clear and understandable.
- Second, the draft Bill will radically overhaul the way these powers are authorised and overseen. It will introduce a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these—and other warrants—cannot come into force until they have been approved by a judge. And it will create a new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.
- Third, it will make sure powers are fit for the digital age. The draft Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. The Government argues that this measure simply restores capabilities that have been lost as a result of changes in the way people communicate.[10]

7. In the lead-up to publication of the draft Bill, there were concerns from various quarters that the new legislation would expand data capture and retention powers beyond the provisions set out in the 2012 draft Communications Data Bill.[11] There were also concerns about whether the draft Bill would attempt to circumscribe the use of encryption in order to facilitate access to communications.

5 Cabinet Office Policy Paper, Queen's Speech 2015: what it means for you, 27 May 2015
6 HC Deb, 11 June 2015, col 1354
7 HC Deb, 11 June 2015, col 1354.
8 David Anderson, A question of trust: report of the Investigatory Powers Review, June 2015
9 HC Deb, 25 June 2015, col 1088
10 Draft Investigatory Powers Bill, Cm 9152, November 2015, p5
11 "Security services' powers to be extended in wide-ranging surveillance bill", Guardian, 27 May 2015

8. In a foreword to the Draft investigatory Powers Bill, the Home Secretary wrote: "The draft Bill only proposes to enhance powers in one area—that of communications data retention—and then only because a strong operational case has been made."[12] With 202 clauses and 9 schedules, the Bill is also to some extent a consolidation measure. Quite to what extent is a point of contention. Dr Richard Clayton, Director of the Cambridge Cloud Cybercrime Centre based in the Computer Laboratory of the University of Cambridge, believed that "the present Bill forbids almost nothing … and hides radical new capabilities behind pages of obscuring detail."[13] In a similar vein, Graham Smith believed that "the suggestion that the new retention power is limited to internet connection records … is open to question",[14] and provided a list of powers in the draft Bill that were in his view either new or greater than those in existing legislation.

Our inquiry

9. Recent events in Paris demonstrate clearly that the ability of law enforcement and security agencies to legally probe the communications of criminals and terrorists has never been more important, which makes getting the Bill right so necessary. Of course, the Bill must balance protecting the law-abiding majority from the criminals and terrorists against protecting the very democratic freedoms these terrorists are seeking to undermine. The right to privacy, embodied in the Human Rights Act 1998, is at the heart of this balance. It is not an absolute right, but one which is qualified to allow for proportionate legal intrusion in order to protect the wider interests of a democratic society. This balancing act will be central to the scrutiny by the Joint Committee on the Draft Investigatory Powers Bill.

10. In our inquiry we have focused on critical technological aspects of the draft Bill. We have not addressed the need or otherwise for the communications monitoring provisions or whether they are proportionate to the threats they are intended to deal with. Our focus has been on how the main technological issues involved might affect the communications businesses that will have to collect data and provide access to the security authorities. If we do not get these technological aspects of the Bill right, not only will the Bill fail to achieve its security objectives but it will also damage our digital economy.

11. Following an initial evidence session on 10 November 2015, we launched our inquiry on 12 November. We called for written evidence on the technical feasibility and costs of meeting the obligations imposed by the Bill; the impact on communications service providers and related businesses; and the likely consequences for people using ICT services. More specifically, we sought views on the extent to which communications data and communications content could be separated and the extent to which this was reflected in the draft Bill, as well as views on encryption, bulk data collection, cloud computing, deep packet inspection and anonymous internet communications systems. We received over 50 written submissions. Following our first oral evidence session on 10 November, during which we heard from industry and academics, we held a second hearing on 8 December with internet businesses and technical experts and the Home Office.

12. We thank all those who have contributed to our short inquiry, including Dr Steven Murdoch of University College London who provided technical advice. We hope that our report, and also the oral and the written evidence we have collected, assists the Joint

12 Draft Investigatory Powers Bill, Cm 9152, November 2015, p1
13 Dr Richard Clayton (IPB0032) para 59
14 Graham Smith (IPB0025) para 29

Committee in its consideration of the draft Bill and the House in considering the proposed Bill itself when it comes forward.

2 Technology issues

13. David Allen Green of Preiskel & Co and legal commentator for the FT commented that the real challenge posed by the draft Bill is whether the measures will work in practice, given developments in technology; and whether overseas communications service providers will cooperate.[15] TechUK identified particular issues of "utmost importance":

- Clear definitions of terms such as "telecommunications service", "relevant communications data", "communications content", "equipment interference", "technical feasibility" and "reasonably practicable";
- Obligations that the draft Bill places on communication service providers (CSPs); in particular overseas providers;
- Further clarification on encryption and equipment interference;
- The technical feasibility of obligations regarding internet connection records.[16]

14. Professor Ross Anderson told us about technological change and the difficulties this could create to the definitions in the Bill:

> … technology just changes too fast. You cannot expect to have a Bill that will last for 25 years unless you have lots of Henry VIII clauses in it and do everything by statutory instrument, which creates problems of its own. The thing that is about to hit us, of course, is the internet of things. The Bill makes some provision for that by talking about things as well as persons, but the true implications of what it means to allow bulk equipment interference, for example, with road vehicles will probably have to be revisited once people start using autonomous vehicles at scale.[17]

Others also highlighted issues around the new 'internet connection records', encryption and equipment interference, which we discuss below.

Internet connection records

What are ICRs?

15. A great deal of attention has been paid to the provisions in the draft Bill for the retention of 'internet connection records' (ICRs). The purpose is to allow law enforcement agencies to identify the communications service to which a device has connected. The Institute for Human Rights and Business commented that "As this is a new provision in the draft Bill, it will require particular scrutiny. There are questions as to how collecting and storing ICRs is technically possible, and whether Data Retention Notices to retain all user ICRs are 'necessary and proportionate'."[18] The Home Office indicated that "we will certainly not place obligations on every one of [the "200 or 300" communications

15 The Investigatory Powers Bill: will it work in practice? 5 November 2015, blogs.ft.com
16 techUK (IPB0037)
17 Q66
18 The Institute for Human Rights and Business (IHRB) (IPB0035)

service providers]".[19] We received a good deal of evidence concerning both the inherent difficulties in defining ICRs and the breadth of the definition in the draft Bill.

16. The draft Bill will require UK communications service providers (CSPs) who are served with a notice to retain internet connection records as 'communications data'. The Home Office define 'communications data' as the 'who', 'when', 'where' and 'how' of a communication, often referred to as its 'metadata'. But it does not include the content of a communication—it does not include every web page that a person has visited, for example, 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 used at any one time, all of which blur the lines between content and metadata. According to Cisco, at present, in order to understand what someone is doing online, CSPs effectively need to track all of the data all the time.[20]

17. New definitions of 'communications data' are given in clause 193 of the draft Bill, on which the Government provides some commentary in the draft Bill publication:

> These new categories are intended to be technology neutral and replace the three categories of communications data in RIPA: 'traffic data', 'service-use data' and 'subscriber data' which no longer adequately reflect the data available from telecommunication operators or systems.[21]

The terms used now are 'entity data' and 'events data'. In addition, clarification around web browsing is given:

> Anything beyond data which identifies the telecommunication service (e.g. bbc.co.uk) is content. Accordingly bbc.co.uk, google.co.uk or facebook.com would be communications data but data showing what searches have been made on Google or whose profiles have been viewed on Facebook would be content.[22]

18. TechUK acknowledged that "the original intention of bringing together various pieces of surveillance legislation into one Bill is to provide clarity to industry, agencies and the public," but were concerned that "over-broad definitions … are counter to this goal", particularly the definitions of what would constitute 'communications data' and 'communications content':

> The definition of "communications data" relates to the "who, what, where, when and with whom" of a communication, yet does not appreciate the vast amounts of metadata that companies would have to retain under the requirements of the draft Bill and the difficulty for companies in separating data (which can be accessed without a warrant) from content (which could not be accessed without a warrant). The extent to which the two can be easily separated requires greater scrutiny—clearer definitions, and acknowledgement of, the metadata in between is therefore required.[23]

19 Q138
20 Cited in House of Commons Library Briefing Paper 7371, Draft Investigatory Powers Bill, 19 November 2015, p21
21 Draft Investigatory Powers Bill, Cm 9152, November 2015, p287
22 Draft Investigatory Powers Bill, Cm 9152, November 2015, p287.
23 techUK (IPB0037)

Exa Networks, an internet service provider, suggested that "some of the definitions of the Bill do not seem to accommodate the complexity of Internet Protocol networks".[24] Philip Virgo, on the other hand, acknowledged a need for enabling legislation to be technology neutral and "to avoid giving too much information to those wishing to avoid investigation", and therefore believed it "unreasonable to expect a detailed list in the Bill of the communications data elements that should be retained."[25]

19. In her statement to the House on 4 November, the Home Secretary said:

> Some have characterised that power as law enforcement having access to people's full web browsing histories. Let me be clear—that is simply wrong. An internet connection record is a record of the communications service that a person has used, not a record of every web page they have accessed. If someone has visited a social media website, an internet connection record will only show that they accessed that site, not the particular pages they looked at, who they communicated with, or what they said. It is simply the modern equivalent of an itemised phone bill.[26]

Some witnesses questioned that analogy. Professor Mike Jackson did not think that "the data we are talking about is the equivalent of an itemised phone bill: It has significantly more information content than an itemised phone bill gives."[27] Dr Joss Wright of the Oxford Internet Institute went further:

> The fundamental issue is that comparing it with telephony is ludicrous. In the modern world, particularly for younger people, a much closer analogy is with the real world. When did you go into your house? When did you leave your house? Which friend did you meet? What shop did you go into? What newspaper did you read? What book did you buy? If we were asking for bulk collection, retention and access to that kind of data in the real world, there would be uproar. Somehow, because this is the internet and it is slotted under "This is just telecommunications," the Bill has got to where it is.[28]

20. In a similar vein, Dr Julian Huppert (a former MP) thought there was very little, if any, difference between ICRs and the 'web logs' considered by the earlier Joint Committee on the 2012 Draft Communications Data Bill, of which he was a member:

> Our report agreed that 'Web logs are at the more intrusive end of the communications data spectrum'. Even though the exact webpage isn't recorded, it would be fairly clear why someone were going to websites such as www.depressionalliance.org.[29]

21. Unlike a phone bill, which clearly and consistently relates to a billed individual, IP addresses are shared by a number of users simultaneously. A communications service provider would ordinarily usually only be able to provide details of the person who pays the internet subscription, which is not necessarily the person who was using a device at a particular time.

24 Exa Networks Limited (IPB0026) para 12
25 Philip Virgo (IPB0031) para 19
26 HC Deb, 4 November 2015, col 970
27 Q69
28 Q69
29 Dr Julian Huppert, University of Cambridge (IPB0027) para 11

22. Graham Smith pointed out that the draft Bill itself uses the term 'internet connection record' only in clause 47 and that this differs from the way in which 'relevant communications data' are defined in clause 71 (which details the powers to require retention of certain data). He described how the scope of 'relevant communications data' depended on thirteen interlinked definitions, and concluded that "the clause 71 power looks as if it may cover a wider range of communications data than is achieved by adding 'Internet Connection Records' to the current list of retainable communications data."[30] He added:

> It would assist the discussion if the Home Office were to provide full, detailed and clear technical information about what data-types it believes would fall within (a) clause 71 and (b) clause 47 and how those would differ from the data-types covered by the existing retention legislation.[31]

Andrews & Arnold made the point that greater clarity and consistency in definitions would "limit the scope of future governments to expand the retention beyond current intentions without a change to the legislation".[32]

23. Some witnesses were concerned about the potential breadth of the ICRs. IT-Political Association of Denmark suggested that "the motivation for ICRs in the draft Bill and the outlined retention requirements are very similar to the session-logging data retention scheme which was used in Denmark from 2007 until 2014, when it was repealed for lack of effectiveness".[33] Open Rights Group considered that the definition used in the Operational Case for the Retention of Internet Connection Records—"a very narrow set of data, such as numerical internet protocol (IP) addresses and port numbers … [and] the time that a specific service was accessed"[34]—does not reflect the definition in the draft Bill. They concluded that "ICRs could be used for a much broader range of purposes than stated in the guidance".[35] They added that:

> ICRs are defined by their use and access regime, and could be understood very narrowly as a list of websites visited or services used, or quite broadly as covering almost all the types of communications data. … The creation of ICRs of web interactions could require the recording of full URLs … [which] would then be edited in order to generate a history of sites visited, which is not as simple as it seems.[36]

24. Richard Alcock from the Home Office assured us that the Government had been engaging very closely with industry, not least on the matter of definitions.[37] The Home Office's Chief Scientific Adviser, Professor Bernard Silverman, thought that the definition of the content of a communication had been pinned down in a way that "satisfies both a legal and a scientific requirement".[38] Richard Alcock emphasised that the purpose for which internet connection records could be used determined the circumstances in which the data could be accessed:

30 Graham Smith (IPB0025) para 10
31 Graham Smith (IPB0025) para 18
32 Andrews & Arnold Ltd (IPB0011)
33 IT-Political Association of Denmark (IPB0051) para 3
34 Home Office, Operational case for the retention of Internet connection records, 4 November 2015
35 Open Rights Group (IPB0034)
36 Open Rights Group (IPB0034)
37 Q120
38 Q126

> One new power that the Bill brings forward relates to what are called internet connection records. In simple terms, that means identifying the communications service that a person was using online at a particular point in time. Of course, what the Bill tries to do is to retain those data relating to individuals, but it also sets out clearly the terms under which the data can be accessed. Those three terms are as follows: one is to identify a person from a particular IP address—an internet protocol address; the second is to identify a person who may have been using an illegal website; the third is to identify what communications service an individual may have been using over time. Those internet connection records cannot be used for any other purpose.[39]

The Home Secretary told us subsequently that the definitions for 'communication data' and ICRs were intended to be "technology neutral and flexible in order that, should user behaviour and technology change, they will still apply".[40] The definitions were to be applied "to the full range of powers and obligations under the draft Bill"[41] which had subsumed provisions from several current statutes. As a result, "the definitions as they are formulated are necessarily abstract".[42]

The feasibility of collecting ICRs

25. The feasibility of collecting, and storing, internet connection records depends on what they actually are. Some ISPs, particularly smaller ones, have expressed concerns about the cost of installing hardware tools to identify and retain ICRs. William Waites described the burdens associated with looking "deep into the packet (known as Deep Packet Inspection or DPI) in order to find what web site is being accessed".[43]

26. TechUK highlighted that many businesses do not already generate or store internet connection records for their business purposes, unlike other types of communications data. An important question was:

> whether it is technically feasible for companies to easily separate 'communications data' from 'communications content' when retaining ICRs. The difficulty that some internet service providers may face during the retention of ICR in separating the first part of the URL up to the first '/' (classified as communications data by the draft Bill and required) from the remainder of the URL after the first '/' (classified as communications content and not required) creates additional complications for businesses.[44]

More fundamentally, James Blessing of the Internet Service Providers Association told us that "the whole idea of an internet connection record does not exist as far as internet service providers are concerned."[45] Andrews and Arnold Ltd, an ISP, said similarly that:

> An ICR does not exist—it is not a real thing in the Internet. At best it may be the collection of, or subset of, communications data that is retained by an

39 Q129
40 Home Office (IPB0065) Annex A
41 Home Office (IPB0065)
42 Home Office (IPB0065).
43 William Waites (IPB0006)
44 techUK (IPB0037)
45 Q3

> operator subject to a retention order which has determined on a case by case basis what data the operator shall retain. It will not be the same for all operators and could be very different indeed. We would like to see the term removed, or at least the vague and nondescript nature of the term made very clear in the Bill and explanatory notes.[46]

27. Matthew Hare of Gigaclear raised a concern about the feasibility of keeping what would be a "massive" volume of ICR data secure:

> There would be the most massive and enormous amount of data that in future an access-provider would be expected to collect and keep, if it received a notice. … All you will do is create a massive database of who uses the internet for what and when, to be stored across a whole range of different service providers to make sure you have the content available, and I would question whether keeping that secure and safe is always going to be the case.[47]

Witnesses provided evidence as to whether there were technological developments which could improve detection of contact data without requiring large volumes of data to be captured, including benefits or otherwise of moving towards 'IPv6'. Witnesses told us that this could potentially improve targeting of data access requests as well as reduce the amount of data required to be stored, although there were challenges to its implementation. James Blessing of the Internet Service Providers Association stated: "IPv6 would make it a lot easier to find people, which is fantastic. Adoption of IPv6 is a bit of a challenge."[48]

28. John Shaw of Sophos had worries about security of the data that would be required:

> There is a requirement to store 12 months' worth of data about the communications. … It is really important that that data itself is then encrypted … Part of the cost is not just collecting the data but making sure that it is then super secure … so that it cannot be used for bad purposes.[49]

Richard Alcock from the Home Office told us that

> In the majority of cases, our data retention stores are completely separate from the business systems that exist within comms service providers. Effectively, they are subject to their own security arrangements. We have very high standards, as you would expect, for the security of the data that we require CSPs to keep.[50]

29. Richard Alcock also explained that the circumstances of particular CSPs would be taken into account:

> In the context of communications data … we work very closely with the comms service providers, even before serving a notice, to understand the technical feasibility, practicality, costs and robustness of the arrangements, noting that in the context of communications data all the data that are retained and used, where necessary and proportionate, have to be built to an evidential standard.

46 Andrews & Arnold Ltd (IPB0011)
47 Q1
48 Q16
49 Q45
50 Q140

> Once that was done, we would serve a written notice, signed by the Home Secretary, on those suppliers, defining the specific fields and data fields that we wished to collect. Those fields will be a function of the different industry suppliers, by virtue of the fact that all the back-office and technical systems are quite different, depending on which comms service provider you are talking to.[51]

Later in our inquiry, the Home Secretary provided us with a detailed list of the types of data that communications service providers might be required to retain in order to generate ICRs and what would constitute 'content',[52] and explained that:

> The Government's proposals regarding ICR retention are the subject of on-going consultation with industry. The Home Office has undertaken technical discussions with academics and industry bodies, as well as with the companies that are most likely to be subject to the obligations under the draft Bill. In light of those discussions, we are confident that the proposals are technically feasible and operationally essential for law enforcement.[53]

The Home Secretary also provided details of the operation of a 'request filter'—a mechanism by which only relevant, and proportionate, information is made available to investigators.

30. **While we are encouraged to learn of the Government's ongoing engagement with the internet industry, there seems still to be confusion about the extent to which 'internet connection records' will have to be collected. This in turn is causing concerns about what the new measures will mean for business plans, costs and competitiveness. Although the Government maintains that ICR notices will be served on particular CSPs on a case by case basis in a way which takes account of the circumstances of the particular communications provider, based on the text of the draft Bill some envisage a situation where ICRs could be required from all CSPs. Given the volume of data involved in the retention of ICRs and the security and cost implications associated with their collection and retention for the CSPs on whom ICR obligations might be placed, it is essential that the Government is more explicit about the obligations it will and will not be placing on industry as a result of this legislation.**

31. ***The Government, in seeking to future-proof the proposed legislation, has produced definitions of internet connection records and other terms which have led to significant confusion on the part of communications service providers and others. Terms such as "telecommunications service", "relevant communications data", "communications content", "equipment interference", "technical feasibility" and "reasonably practicable" need to be clarified as a matter of urgency. The Government should review the draft Bill to ensure that the obligations it is creating on industry are both clear and proportionate. Furthermore, the proposed draft Codes of Practice (which we discuss in paragraph 69 below) should include the helpful, detailed examples that the Home Office have provided to us.***

51 Q134
52 Home Office (IPB0065) Annex B
53 Home Office (IPB0065)

Encryption

32. With the commencement of Part I Chapter II, and (in 2007) Part III of the Regulation of Investigatory Powers Act 2000, the Interception of Communications Commissioner was given further responsibilities for overseeing notices ordering the decryption of data acquired by interception and the adequacy of arrangements for the protection of communications data and encryption keys for intercepted material.

33. Many witnesses emphasised the importance of the use of encryption in providing the secure internet environment we need for many services, from credit cards and commerce, patient data and medical information, proprietary business and legal discussions, and other important communications.[54] Before the draft Bill was published, there was speculation that it would address the use of encryption software. Professor Mike Jackson of Birmingham City University postulated that one approach would have been to legislate against the use of complex encryption that government bodies could not break, but noted that the "problem with this approach is that if the security forces can break the encryption then hackers will as well".[55] When the draft Bill was finally published, on 4 November, the Government stated that the Bill "will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA".[56]

34. Clause 189 of the draft Bill, however, provides that the Secretary of State can use regulations to impose obligations on CSPs, via "technical capability notices". 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 communications service-user rather than the service-provider, so that the service-provider cannot 'see' the message content. Andrews & Arnold Ltd believed that:

> Over the next few years it is likely to become quite rare for a web site to be unencrypted. At present some level of deep packet inspection can find the website name of an encrypted website from the initial negotiation, but this loophole is being plugged in the more modern protocols. This calls in to question the whole justification for logging 'internet connection records'.[57]

35. Privacy International were concerned about clause 189 (4)(c) of the draft Bill which could impose "obligations relating to the removal of electronic protection applied by a relevant operator to any telecommunications or data".[58] These obligations are on top of those placed on telecommunications services to assist in "giving effect" to interception warrants (Clause 31) and other similar clauses elsewhere in the Bill. Privacy International told us that these, and other clauses, were "an indirect attack on end-to-end encryption, which the Government has previously stated it would not undermine."[59]

54 E.g. Mozilla (IPB0056)
55 "'Profoundly wrong' Investigatory Powers Bill slammed for 'treating everyone as a suspect'", Computing, 28 May 2015
56 Draft Investigatory Powers Bill, Cm 9152, November 2015, p29
57 Andrews & Arnold Ltd (IPB0011)
58 Privacy International (IPB0040) para 24
59 Privacy International (IPB0040) para 24.

36. Others had similar concerns, including TechUK, the Institute for Human Rights and Business and Mozilla. TechUK told us:

> Although the Government has been at pains to stress that it is not restricting or weakening encryption, and that all requirements in the Bill regarding the 'removal of electronic protection' are already provided for in current legislation, further scrutiny around this is needed.[60]

They wanted, in particular, the envisaged 'technically feasible' test for the 'removal of electronic protection' to include a consideration of whether it was "reasonable and proportionate":

> It should be noted that Clause 190 states that the Secretary of State, before giving a notice relating to the removal of electronic protection, would have to consider the 'technical feasibility' of complying with such a notice. For the test of whether a measure is 'technically feasible' to be meaningful, it must consider something more than whether the end result is technically achievable with sufficient engineering manpower, investment and time … The consideration as to whether a measure is technically feasible should also consider whether the time, cost (including opportunity cost), knock-on effects and change in customer relationships are reasonable and proportionate to the expected benefits.[61]

37. The Institute for Human Rights and Business suggested that, while it was likely that the draft Bill would not eliminate end-to-end encryption, "it will prevent companies served with a technical capability notice from offering end-to-end encryption as part of their services".[62] The obligations on the 'removal of electronic protection' by clause 189 (4) (c) were, they said, "widely believed to refer to end-to-end encryption, where no actor holds the 'keys' to decrypt communications and are therefore impossible to intercept."[63] Mozilla similarly saw the draft Bill permitting "backdoor mandates" through the obligations imposed by a "maintenance of capability order," which might include an obligation to "remove the electronic protection". They thought the Bill could be used:

> to compel a software developer, like Mozilla, to ship hostile software, essentially malware, to a user—or many users—without notice. As an open source project, this is problematic from both philosophical and practical perspectives.[64]

Recently, Apple and other communications companies have expressed concerns about whether the draft Bill might require them to adopt weaker standards of encryption. Apple have also reportedly stated that the draft Investigatory Powers Bill could be a catalyst for other countries to enact similar measures, leading to significant numbers of contradictory country-specific laws.[65]

60 techUK (IPB0037)
61 techUK (IPB0037)
62 The Institute for Human Rights and Business (IHRB) (IPB0035)
63 The Institute for Human Rights and Business (IHRB) (IPB0035) . para 4.2
64 Mozilla (IPB0056) para 3.3
65 "Apple launches Silicon Valley fightback over surveillance bill", Financial Times, 22 December 2015

38. The IT-Political Association of Denmark suggested that wrong-doers might take additional steps, such as the use of anonymity tools like virtual private networks and Tor,[66] to protect their privacy as knowledge of the surveillance capabilities of the police and security services improved. Dr Joss Wright of the Oxford Internet Institute foresaw "chilling effects" that awareness of surveillance might have on even the legitimate web browsing activities of consumers.[67]

39. While publication of the draft Bill might have highlighted industry's concerns over encryption, Dr Julian Huppert reminded us that there is already legislation that allows communications providers to be required to maintain an ability to provide the content of communications unencrypted.[68] However, he raised a question about enforceability: "It is unclear what would happen if a court were to be asked to take action against an operator who was unable to comply with this power because of the fundamental nature of their product: Any decentralised communications system is likely to render this clause impossible to comply with."[69] Dr Robert Nowill of Herne Hill Consulting told us that ISPs and CSPs could "unwrap" encryption which they themselves had put in place, but that "if the underlying data stream is encrypted by something proprietary and unknown and is originating and terminating overseas, you would probably have the devil of a job digging into it".[70]

40. Whether someone sufficiently determined to communicate in an encrypted fashion would be able to do so unbreakably is a moot point.[71] Professor Sir David Omand suggested that this should not stop us from trying to see their communications when criminals or terrorists are involved:

> Criminals don't normally conduct their crime by breaking the encryption anyway, but do you want deliberately to remove what I would describe as the right to seek on the part of the police and the intelligence agencies—to try to find out if they can get a lead on some terrorist group, criminal group or paedophile network? We should be encouraging them to try, but there is no guarantee. I am certainly not advocating back doors being mandated, things which would weaken the integrity of the internet; there is a lot of nonsense talked about all of that. But they have to try, and some of the Bill would enable one or two tricks of the trade to be applied. Computer interference is one of those, which might give them a chance to get across some of the most dangerous people who are out there. I don't think you can ask for more than that.[72]

41. When we questioned our Home Office witnesses about how encrypted communications would be dealt with under the draft Bill, they told us that the expectation would be that communications service providers would submit content data, when ordered to do so, "in the clear"—that is unencrypted—and that this was the same as was currently required under Regulation of Investigatory Powers Act 2000.[73] However, that would not apply to

66 The Onion Router
67 Q75
68 Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 (SI 2002/1931) para 10 of the schedule.
69 Dr Julian Huppert, University of Cambridge (IPB0027) para 27
70 Q155
71 Q43
72 Q87
73 Q135

content that is encrypted end-to-end before being passed to the communications provider for transmission: "What has to be removed is the electronic protection that the service-provider itself has put on the message. It is not removing encryption; it is removing electronic protection."[74]

42. ***In tightly prescribed circumstances, law enforcement and security services should be able to seek to obtain unencrypted data from communications service providers. They should only seek such information where it is clearly feasible, and reasonably practicable, and where its provision would be consistent with the right to privacy in UK and EU law. The obligations on potential providers of such data should be clarified in the proposed Codes of Practice to be published in draft alongside the Bill later this year (paragraph 69).***

43. ***There is some confusion about how the draft Bill would affect end-to-end encrypted communications, where decryption might not be possible by a communications provider that had not added the original encryption. The Government should clarify and state clearly in the Codes of Practice that it will not be seeking unencrypted content in such cases, in line with the way existing legislation is currently applied.***

Equipment interference

44. 'Equipment interference' allows the security and intelligence agencies, law enforcement and the armed forces to target electronic equipment such as computers and smartphones in order to obtain data, including communications content. Equipment interference encompasses a wide range of activity from remote access to computers to downloading covertly the contents of a mobile phone during a search.

45. Clause 99 of the draft Bill includes obligations on domestic CSPs to assist in giving effect to equipment interference warrants. Clause 101 explicitly applies this duty to 'relevant telecommunications providers'. Privacy International explained their concerns about these provisions:

> Under these two clauses, communications service providers could be compelled to take any steps, unless 'not reasonably practicable', to assist the police and the intelligence services to hack our computers and other devices. While we do not know what this assistance might look like in practice, it could include compelling communication service providers to send false security updates to a consumer in order to install malware that the police or intelligence services could then use to control the consumer's computer.[75]

46. Professor Ross Anderson acknowledged the value of equipment interference provided that it was targeted, but also had concerns about the way it might be applied in practice:

> The right way to get round encryption is targeted equipment interference, and that is hack the laptop, the phone, the car, the Barbie doll or whatever of the gang boss you are going after, so that you get access to the microphones, to the cameras and to the stored data. The wrong way to do it is bulk equipment interference.[76]

74 Q154
75 Privacy International (IPB0040) paras 20-21
76 Q88

> The draft Bill gives intelligence and law-enforcement agencies hacking powers ('equipment interference') that are excessive, and that need to be much more tightly controlled. As the Bill stands, its equipment interference provisions are likely to damage both national security and British industry.[77]

47. Some of the perceived difficulties with equipment interference relate to the definitions. TechUK commented:

> Within the draft Bill, the term 'equipment' is defined as any equipment "producing electromagnetic, acoustic or other emissions, or any device capable of being used in connection with such equipment". This term is particularly vague … Would, for example, an autonomous vehicle fall under this definition?[78]

Another difficulty could be the potential extent of these provisions. The Electronic Frontier Foundation were worried that the only qualification to equipment interference order is clause 101(6), which removes the requirement where any steps would not be "reasonably practicable". The Foundation noted that there is "no guidance as how 'reasonably practicable' may be determined".[79] Big Brother Watch took little comfort from a *draft Code of Practice on Equipment Interference*, published on 4 November under section 71(4) of the Regulation of Investigatory Powers Act 2000, because there remained a need to clarify "loose and unexplained wording".[80]

48. Some of our witnesses suggested that there could be technical difficulties associated with at least some approaches to equipment interference. The Electronic Frontier Foundation believed that software updates intended as methods of surveillance could be identified as such.[81] Big Brother Watch noted that weakening a system does not mean that only law enforcement or the intelligence agencies can exploit it—"The system can be exploited by anyone who uncovers the weakness, including malicious actors, rogue states or non-Government hackers".[82]

49. There are other challenges connected with the ever-growing deployment of 'open source' software. Antony Walker of TechUK told us:

> Potentially there are significant problems for companies based fundamentally on an open source business model. … The very nature of [Mozilla's] business, which is based on inputs from the open source community, means that a lot of its code has to be out in the open. Therefore, meeting any of the equipment interference requirements would be something it could not conceal from the people who provide the open source software. A company like that would face very real specific problems.[83]

Stan Shapiro was concerned that third parties—hackers, scammers or web developers—could insert malicious records into a web-browsing history, with "no way to resolve which records are genuine and which are malicious retrospectively".[84]

77 Professor Ross Anderson (IPB0036)
78 techUK (IPB0037)
79 Electronic Frontier Foundation (IPB0017) para 10
80 Big Brother Watch (IPB0048)
81 Electronic Frontier Foundation (IPB0017) paras 23-24
82 Big Brother Watch (IPB0048)
83 Q 101
84 Stan Shapiro (IPB0057)

50. **The Government states that the draft Bill introduces no substantive changes to the existing 'equipment interference' regime. It has made the practices more visible to the public and industry, however, and it remains to be seen whether this greater visibility affects the nature or extent of such activity in practice. Some sectors of the communications industry have concerns that equipment interference could jeopardise their business model; for example those producing and distributing open source data. They have a concern that because, as now, CSPs will not be permitted to reveal any equipment interference, their clients may assume that it is used.**

51. ***As ever, the fight against serious crime should be appropriately balanced with the requirement to protect and promote the UK's commercial competitiveness. We believe the industry case regarding public fear about 'equipment interference' is well founded. The Investigatory Powers Commissioner should carefully monitor public reaction to this power and the Government should stand ready to refine its approach to 'equipment interference' if these fears are realised. Taking into account security considerations, the Investigatory Powers Commissioner should report to the public on the extent to which such measures are used.***

3 Impacts on communications businesses

52. Before the publication of the draft Bill, the Internet Service Providers Association (ISPA) called for full consideration to be given to the impact on business:

> Software, IT and telecoms services together generated 4.2% of UK gross value added (£59bn) in 2011 and provided 885,000 jobs … We call on all parliamentarians to ensure that the Investigatory Powers Bill does not put competiveness of the UK economy at a disadvantage. Online and digital business recognise their responsibilities but the impact of any new provision in the Bill needs to be clearly considered and costed.[85]

53. Many of our witnesses have raised issues about the technical feasibility and cost of the Bill's measures. A globalised communications industry depends on the inherent globalised nature of the internet itself. The potential for differing—conflicting, even—national laws raises compliance issues and increases uncertainty for businesses. With compliance comes cost. We heard concerns, for example, about the potential costs associated with storing large amounts of data. Many complained about a lack of clarity in some definitions and terms.

54. Others worried about the potential knock-on effects for UK industry, such as those using open source software (paragraph 49). The Internet Infrastructure Coalition noted that "Those seeking to start businesses, or relocate them, look closely at whether the laws in a country are 'tech positive' and encourage the kind of innovation and imagination necessary to create a new business."[86] Matthew Hare of Gigaclear told us that:

> The UK relies on the information industries in their broadest sense, from financial services through legal to software and gaming; it affects everyone in the information industry. If we make it appear that this is a worse place to do business, because of some rights that, as far as most of us know, the Government never take up—but we will never know because we are not even allowed to talk about it—it seems to me a massive own goal.[87]

Some saw potential for a commercially chilling effect for the UK. Exa Networks, an internet service provider, believed that "the Bill would weaken and worsen the competitiveness of the UK technology industry as it affects privacy protection, such as encryption, and the ability to use equipment free of interference".[88]

55. BT considered that it was "appropriate to maintain a regime that permits access to content and communications data, provided that the circumstances are suitably circumscribed, and provided that all necessary checks and balances are in place to ensure the lawful and proportionate operation of that regime",[89] but BT's Mark Hughes wanted clarity that "the Bill and the law should apply where we provide public networks, not

85 ISPA, Investigatory Powers Bill – Parliamentary Checklist, 2 November 2015
86 Internet Infrastructure Coalition (I2Coalition) (IPB0015) para 8
87 Q 31
88 Exa Networks Limited (IPB0026) para 5
89 BT (IPB0061)

private networks".[90] The Electronic Frontier Foundation pointed out that the draft Bill's expansion of the definition of 'telecommunications service' (first introduced in the Data Retention and Investigatory Powers Act) means that even within the realm of 'public networks' individual internet services such as Facebook, Twitter, Dropbox, Microsoft Office Online, and others would now be included in the definition.[91] Graham Smith wanted clarity about whether an 'internet communications service' was intended to be limited to human-to-human messaging.[92]

56. TechUK were concerned that business models might have to be changed. They worried that powers in the draft Bill, under Clause 71(8)(b), requiring retention of data by "collection, generation or otherwise" suggest that "the Government reserves the right to compel companies to change their business models in order to facilitate access to data that they would not have kept under standard business operations".[93]

57. Several witnesses expressed concern about the potential impact on businesses of the Bill's requirement for internet connection records. BT noted that "many of the powers contained in the Bill (e.g. lawful interception and obtaining of communications data) are derived from those already contained in RIPA and other associated legislation: These are well understood and should not pose difficulties from a technical perspective."[94] However, on the need for internet connection records, they cautioned that:

> Whilst the concept of an ICR may seem relatively straightforward, the introduction of a capability to retain them will be less so. … BT does not currently generate (or retain) a single set of data that is capable of meeting the proposed requirement. We are currently scoping what data sources and methods we could employ to generate ICRs.[95]

John Shaw of Sophos told us: "The crucial difference with the new Bill is the requirement to hold 12 months of data on everyone all the time … It is not just the cost of the data; the exposure of everyone in the UK's data to people trying to hack it to do bad things with it is a very meaningful difference".[96] BT reckoned that without further information "we cannot realistically scope technical feasibility or cost".[97]

58. Below we discuss the particular potential impacts for communications businesses in terms of cost and compliance.

Costs

59. According to the Government, the only additional costs on communications service providers relate to the obligations that may be imposed on them for collecting internet connection records. It estimates the figure at £174.2 million in discounted net present value terms over the next 10 years,[98] but there was uncertainty among the communications technical community on whether this would cover all the associated

90 Q92
91 Electronic Frontier Foundation (IPB0017) para 27
92 Graham Smith (IPB0025) para 25
93 techUK (IPB0037)
94 BT (IPB0061)
95 BT (IPB0061)
96 Q21
97 BT (IPB0061)
98 Home Office (IPB0065)

costs. BT was "not clear on what basis Government has decided to set aside £175m towards the costs of retaining ICRs."[99] JISC (which provides digital technology and resources to higher education, further education and researchers) told us that the costs arising from the Bill would depend on the extent to which the Secretary of State chooses to exercise her "wide powers".[100] The Home Secretary told us that the cost estimates set out in the Impact Assessments published alongside the draft Bill "continue to be refined in consultation with the companies that are likely to be subject to obligations under the Bill".[101]

60. James Blessing of the Internet Service Providers Association (ISPA) calculated that "the Bill appears to be limiting the amount of funds available to a figure we do not recognise as one that would be suitable for the entire industry to be able to do it."[102] Andrews & Arnold Ltd told us of concerns among smaller ISPs that they could be subject to a retention notice which could require 'deep packet inspection' to produce the ICR, and which might have significant cost implications.[103] Another ISP, Exa Networks, worried that technologies permitting the categorisation of the information in order to extract metadata only, are "extremely expensive, as they need to work on all the information passing through the network".[104]

61. The bulk of the cost associated with ICRs relates to the capital costs of providing storage. We discussed above how witnesses had concerns about the feasibility of holding and keeping secure the "massive" volume of data involved (paragraph 27). Those concerns were as much about the costs involved as about technical and security issues. The draft Bill provides for CSPs to make representations to the Technical Advisory Board (which we discuss below).[105] Richard Alcock from the Home Office told us that:

> The fall-back, if there is a disagreement, is to go through the Technical Advisory Board, which will have considered the technical implementation. If it was not possible for a particular organisation to implement things for a certain cost, that would be addressed through the TAB.[106]

62. Clause 185 of the draft Bill provides that CSPs receive an "appropriate contribution" towards their compliance costs. As drafted, the clause promises that this contribution will "never be nil." The IT-Political Association of Denmark told us how in that country the equipment cost of data retention systems is borne by the telecommunications companies (with access to the data billed to the police). If costs in the proposed UK system were not fully covered by the Government, a likely "substantial fixed element [of costs remaining with the companies] would effectively discriminate against smaller ISPs and new companies that consider entering the ISP business".[107]

63. BT told us that "to ensure competitive fairness … it is imperative for the new regime to apply a level playing field for all providers of communications services in the UK. And we believe that it should be made expressly clear that all eligible costs incurred by those

99 BT (IPB0061)
100 Jisc (IPB0012) para 4
101 Home Office (IPB0065)
102 Q6
103 Andrews & Arnold Ltd (IPB0011)
104 Exa Networks Limited (IPB0026) para 25
105 See clause 73 (Review by the Secretary of State)
106 Q145
107 IT-Political Association of Denmark (IPB0051) para 24

providers should be met by Government."[108] This is the view across businesses of all sizes. Andrews & Arnold Ltd told us that they had received indications from the Home Office that operators, as now, would receive 100% cost recovery.[109] Richard Alcock from the Home Office assured us that so far the Government had indeed paid 100% of the costs "relating to implementation".[110] However, the Home Secretary appeared reluctant to include such a commitment on the face of the Bill when it comes forward:

> The Government recognises that the obligations imposed on communications service providers incur additional cost and would not want those subject to such obligations to be put at commercial disadvantage. The Government's current policy, and that of its predecessors, is that it would not be appropriate to expect companies to meet the costs themselves and that they will receive an appropriate contribution towards the costs of obligations in respect of both communications data and interception. The draft Bill maintains the position that CSPs should receive an appropriate contribution in respect of their costs in complying with the legislation.
>
> Cost recovery arrangements are a matter of policy for the Government of the day. It would not be appropriate to tie future Governments to the existing policy by placing these arrangements on the face of the legislation.[111]

64. Apart from ICR costs, some costs are also envisaged for the operation of a 'request filter' which will be established and maintained by the Home Office (although there is provision to transfer its functions to another public authority).[112] This is expected to cost £12.9m in discounted net present value terms over the next 10 years. Clauses 51–53 of the draft Bill would allow the Government to establish a filter system whereby when a complex request for communications data is made 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. The Open Rights Group describes the filter as one of the most concerning aspects of the draft Bill in that it "would allow the police and authorised public bodies to search and analyse retained communications data".[113]

65. ***Given the speed with which this legislation must be in force, the Government must work with industry to improve estimates of all of the compliance costs associated with the measures in the draft Bill, for meeting ICR-related and other obligations, as a matter of urgency. Should the measures in the draft Bill come into force, it will be important for Parliament to have access to information on actual costs incurred in order to assess the proportionality and economic impact of the investigatory powers regime and its effectiveness.***

66. ***Larger CSPs may be able to take some assurance from the Government's commitment to meet their "reasonable" costs and avoid putting any affected businesses "at commercial disadvantage". However, smaller CSPs may not be certain that they will be served with a notice to collect ICRs and, if they do have to, whether their costs will in fact meet the Government's 'reasonable costs' criteria for reimbursement.***

108 BT (IPB0061)
109 Andrews & Arnold Ltd (IPB0011)
110 Q144
111 Home Office (IPB0065)
112 Home Office (IPB0065) Annex B
113 Open Rights Group (IPB0034)

The Government should reconsider its reluctance for including in the Bill an explicit commitment that Government will pay the full costs incurred by compliance.

Compliance

67. Clauses 29–31 of the draft Bill deal with the issuing and serving of warrants, and impose a duty on operators to assist with their 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'. Engagement with overseas companies has to date been on an entirely voluntary basis.[114]

68. Mark Hughes of BT told us that:

> Anyone providing services in the UK will come under the Investigatory Powers Bill, wherever they are located, and should do according to the draft legislation. However, there could be issues associated with those who provide services in the UK but are not located in the UK. Clearly, jurisdictionally, getting them to comply if they are located overseas is a clear challenge; a request from the UK may conflict with local laws.[115]

He did not think however that large ISPs based in the UK would be prompted by the legislation to re-locate overseas. The same might not be true of all ISPs. The Internet Infrastructure Coalition were concerned that those seeking to start businesses will look closely at whether the laws in this country are "tech positive" (paragraph 54).

69. The Royal United Services Institute's *Independent Surveillance Review* concluded that 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).[116] Clause 179 of the draft Bill provides for the Secretary of State to issue Codes of Practice governing the use of powers contained in the Bill. The Home Office told us that draft Codes of Practice will be published alongside the Bill itself when it is introduced.[117] Mark Hughes of BT noted the need for a forum for:

> robust exchanges in understanding some of the matters we are dealing with here: for example, how one can practically work through and then issue of codes of practice, which are important, and have examples before getting into issuance of either a technical capability notice or a data retention order, which obviously is the net result of the Bill being enacted.[118]

70. Professor Sir David Omand also explained the importance of such Codes of Practice:

> If you try to nail everything down absolutely in the primary legislation, you will be revisiting this in a couple of years' time and passing another Investigatory Powers Act. The answer is to learn from the mistake that the Home Office made over the last five years, which was not to update the Codes of Practice, so

114 David Anderson, A question of trust: report of the Investigatory Powers Review, June 2015 (para 11.18)
115 Q101
116 Royal United Services Institute, A Democratic Licence to Operate: Report of the Independent Surveillance Review, 13 July 2015
117 Home Office (IPB0065), Annex A
118 Q110

> that we, the citizens, knew how the existing legislation was being used. They could have done that, in which case the Snowden case would not have been the shock, horror that apparently it was for many people. Those Codes of Practice are presented to Parliament. You can insist that they are revised. You could put that in your legislation. There are ways in which the Government at any one time can be quite precise about how it is interpreting them, which will help the judges very considerably. That can then be updated.[119]

71. ***The Government intends to publish draft Codes of Practice when it introduces the Bill itself, later this year. It is essential that this timetable does not slip and that the Codes of Practice are indeed published alongside the Bill so they can be fully scrutinised and debated. The Government should reduce uncertainty about compliance burdens for businesses, proportionality and about cost recovery, by explicitly addressing such issues in the Codes of Practice. These Codes of Practice should clearly address the requirements for protecting ICR data that will have to be retained and managed by CSPs, along with the security standards that will have to be applied to keep them safe. Businesses based in the UK and those serving UK customers should not be placed at a commercial disadvantage compared with their overseas competitors.***

72. ***Detailed Codes of Practice will be needed to provide a more effective means of assisting compliance, and retaining business confidence in the feasibility of investigatory powers provisions, and their regular updating should be an explicit requirement in the Bill when it is introduced. Specifically, the Bill should require that at regular set intervals (perhaps yearly) the Technical Advisory Board (paragraph 79) is consulted about keeping the Codes of Practice up to date—a new role we propose for that body—and allowing both the Government and business representatives to bring forward amendments.***

Consultation and technical advice

73. In 2012, the Joint Committee set up to scrutinise the Draft Communications Data Bill recommended that there should be much better consultation with industry, technical experts, civil liberties groups, public authorities and law enforcement bodies before any new Bill was introduced. The Intelligence and Security Committee also published a report in 2013 raising similar concerns, including that there had been insufficient consultation with CSPs.[120] For the current draft Investigatory Powers Bill, the Home Secretary told us:

> Over several months, policy officials have engaged with technical experts, both within the Home Office and externally, communication service providers and wider industry, and academics, to inform the drafting of the Bill. This consultation is ongoing, and has informed both the policy development process, and also the drawing up of costs and impact on business as set out in the accompanying Bill documentation.[121]

74. The vagueness of definitions and terms have been a constant feature in the evidence we have taken (paragraph 47). Martin Kleppmann found it understandable that, as he

119 Q66

120 Intelligence and Security Committee, Access to communications data by the intelligence and security Agencies, Cm 8514, February 2013

121 Home Secretary (IPB0030)

saw it, the Government did not wish to specify technical matters in fine-grained details, "since those details may be rendered obsolete by rapid shifts in technology, forcing the law to constantly catch up".[122] But he complained that:

> The current proposed Bill errs too far on the side of generality: its widely criticised "fuzzy definitions" are open to wide-ranging interpretation, leaving technology implementers in doubt as to the legal status of their software, and deferring the important questions of interpretation to executive decisions by the government or to case law.[123]

75. **From the evidence we have received, it is clear that the Home Office has engaged with communications businesses and the wider internet community. *This should remain a central strand of the Government's strategy to ensure effective implementation and for seeking to allay concerns over current uncertainties and confusion arising from the way some terms are defined in the draft Bill. (We have separately recommended clarifying definitions and strengthening consultation processes through the Technical Advisory Board (paragraph 79) once the Bill is enacted.)***

76. **Internet businesses and their users require assurances that investigatory powers will be imposed proportionately, and that the judgement as to what is proportionate should at all times be open to reasonable challenge. The proposed Investigatory Powers legislation, to the extent that it consolidates and clarifies mostly existing provisions, is itself an important response to that requirement. *The Government should continue to consult and explain fully the likely implications of the proposed legislation.***

77. The Royal United Services Institute's *Independent Surveillance Review* recommended that the existing Technical Advisory Board should be replaced with an Advisory Council for Digital Technology and Engineering, which would be a statutory non-departmental public body.[124] The Advisory Council, it concluded, 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.

78. In the context of the potential requirements to store large amounts of communications data, we were told by the Internet Infrastructure Coalition that "small to medium sized Internet infrastructure providers must be included in the Technical Advisory Boards contemplated by the Draft Bill."[125] The Home Office's Chief Scientific Adviser, Professor Bernard Silverman, thought that in principle the idea of a "broadly based advisory board is important, but it is key that its terms of reference should be properly laid out".[126] He added:

> If you have a technical advisory board and it is going to mission-creep into legal issues, it is much better that it should have proper, formal legal terms of reference, rather than that it should be a scientific advisory board that then decides that it will have opinions about commercial and legal things.[127]

122 Martin Kleppmann (IPB0033) para 3
123 Martin Kleppmann (IPB0033) para 3.
124 Royal United Services Institute, A Democratic Licence to Operate: Report of the Independent Surveillance Review, 13 July 2015
125 Internet Infrastructure Coalition (I2Coalition) (IPB0015)
126 Q122
127 Q122

It would be a good idea, he told us, to have in place protocols to cover situations where members of the Board were in dispute.[128]

79. Clauses 181–183 of the draft Bill provide for oversight and advisory functions in relation to the retention of communications data under Part 4 of the Bill, including the continued operation of a Technical Advisory Board. The Technical Advisory Board currently comprises 13 people: six representatives of communications service providers, six representatives of the intercepting agencies and an independent Chair. The Home Secretary told us that it is the Government's intention to maintain the size and balance of the TAB.[129]

80. ***The Government should review the composition of the Technical Advisory Board to ensure that it will have members from industry who will be able to give proper consideration, not just to the technical aspects of appeals submitted to it from CSPs concerned about ICR or other interception or 'interference' notices, but also any concerns raised about costs (paragraph 61). The Government should also produce an explicit framework for how mediation of disputes and challenge will be resolved. The Government should consider whether the Board will need stronger legal expertise in light of the new investigatory powers that it will have to deal with. Membership of the Board should also more generally reflect a wide range of internet industries and expertise, and be able to co-opt individuals from individual businesses likely to be directly affected.***

81. ***The Government did not set up the 'Advisory Council for Digital Technology and Engineering' advocated by the Royal United Services Institute. It should nevertheless add to the remit of the Technical Advisory Board a role it envisaged for that Council—to keep under review the domestic and international implications of the evolution of the internet, digital technology and infrastructure.***

128 Q146
129 Home Office (IPB0065), Annex C

4 Our conclusions and the Joint Committee

82. The draft Investigatory Powers Bill addresses issues of fundamental importance for the country's security, but also for the burdens that will arise from it—those that will be placed on communications businesses and those on law-abiding people who may suffer a loss of privacy. Technology is at the heart of the way the draft Bill's provisions will be implemented, and felt. On that basis our inquiry has focussed on the technology issues, including practicality issues and the extent to which the burdens of technology-centred processes and costs will arise and be dealt with. Our conclusions about these matters are inevitably founded on a moving situation, with some details still being negotiated by the Government with communications industry representatives and other details being aired as the Joint Committee's larger inquiry progresses.

83. We have not addressed the wider ethical issues involved, which we anticipate will feature in the Joint Committee's inquiry and report. We have not considered, specifically, the security need or otherwise for the communications monitoring provisions in the draft Bill, nor whether they are proportionate to the threats that they are intended to deal with. We noted for example the increasing difficulty there will be in distinguishing between communications 'data' (which some CSPs will have to collect for ICRs) and communications 'content' (which they will not), but we have not examined the justification or otherwise for the degree of intrusiveness that collecting communications data will bring. We have not addressed the extent to which, as the Government imply, provisions on encryption are substantially new or merely consolidate existing law and the practices of the security authorities. Instead, we have examined the consequences for communications providers. We have described the way the provisions on 'equipment interference' hinge on definitions that are unclear and may have impacts on communications companies that use 'open source' data, but we have not examined whether the draft Bill changes the way the authorities use "tricks of the trade"[130] to get access to devices and their communications.

84. Our findings—along with the evidence we have collected—focus on the technology aspects that the Joint Committee, we hope, will wish to take into account as it examines all aspects of the draft Bill.

130 Q87

Conclusions and recommendations

Technology issues

1. While we are encouraged to learn of the Government's ongoing engagement with the internet industry, there seems still to be confusion about the extent to which 'internet connection records' will have to be collected. This in turn is causing concerns about what the new measures will mean for business plans, costs and competitiveness. Although the Government maintains that ICR notices will be served on particular CSPs on a case by case basis in a way which takes account of the circumstances of the particular communications provider, based on the text of the draft Bill some envisage a situation where ICRs could be required from all CSPs. Given the volume of data involved in the retention of ICRs and the security and cost implications associated with their collection and retention for the CSPs on whom ICR obligations might be placed, it is essential that the Government is more explicit about the obligations it will and will not be placing on industry as a result of this legislation. (Paragraph 30)

2. *The Government, in seeking to future-proof the proposed legislation, has produced definitions of internet connection records and other terms which have led to significant confusion on the part of communications service providers and others. Terms such as "telecommunications service", "relevant communications data", "communications content", "equipment interference", "technical feasibility" and "reasonably practicable" need to be clarified as a matter of urgency. The Government should review the draft Bill to ensure that the obligations it is creating on industry are both clear and proportionate. Furthermore, the proposed draft Codes of Practice should include the helpful, detailed examples that the Home Office have provided to us.* (Paragraph 31)

3. *In tightly prescribed circumstances, law enforcement and security services should be able to seek to obtain unencrypted data from communications service providers. They should only seek such information where it is clearly feasible, and reasonably practicable, and where its provision would be consistent with the right to privacy in UK and EU law. The obligations on potential providers of such data should be clarified in the proposed Codes of Practice to be published in draft alongside the Bill later this year.* (Paragraph 42)

4. *There is some confusion about how the draft Bill would affect end-to-end encrypted communications, where decryption might not be possible by a communications provider that had not added the original encryption. The Government should clarify and state clearly in the Codes of Practice that it will not be seeking unencrypted content in such cases, in line with the way existing legislation is currently applied.* (Paragraph 43)

5. The Government states that the draft Bill introduces no substantive changes to the existing 'equipment interference' regime. It has made the practices more visible to the public and industry, however, and it remains to be seen whether this greater visibility affects the nature or extent of such activity in practice. Some sectors of the communications industry have concerns that equipment interference could jeopardise their business model; for example those producing and distributing open

source data. They have a concern that because, as now, CSPs will not be permitted to reveal any equipment interference, their clients may assume that it is used. (Paragraph 50)

6. *As ever, the fight against serious crime should be appropriately balanced with the requirement to protect and promote the UK's commercial competitiveness. We believe the industry case regarding public fear about 'equipment interference' is well founded. The Investigatory Powers Commissioner should carefully monitor public reaction to this power and the Government should stand ready to refine its approach to 'equipment interference' if these fears are realised. Taking into account security considerations, the Investigatory Powers Commissioner should report to the public on the extent to which such measures are used.* (Paragraph 51)

Impacts on communications businesses

7. *Given the speed with which this legislation must be in force, the Government must work with industry to improve estimates of all of the compliance costs associated with the measures in the draft Bill, for meeting ICR-related and other obligations, as a matter of urgency. Should the measures in the draft Bill come into force, it will be important for Parliament to have access to information on actual costs incurred in order to assess the proportionality and economic impact of the investigatory powers regime and its effectiveness.* (Paragraph 65)

8. *Larger CSPs may be able to take some assurance from the Government's commitment to meet their "reasonable" costs and avoid putting any affected businesses "at commercial disadvantage". However, smaller CSPs may not be certain that they will be served with a notice to collect ICRs and, if they do have to, whether their costs will in fact meet the Government's 'reasonable costs' criteria for reimbursement. The Government should reconsider its reluctance for including in the Bill an explicit commitment that Government will pay the full costs incurred by compliance.* (Paragraph 66)

9. *The Government intends to publish draft Codes of Practice when it introduces the Bill itself, later this year. It is essential that this timetable does not slip and that the Codes of Practice are indeed published alongside the Bill so they can be fully scrutinised and debated. The Government should reduce uncertainty about compliance burdens for businesses, proportionality and about cost recovery, by explicitly addressing such issues in the Codes of Practice. These Codes of Practice should clearly address the requirements for protecting ICR data that will have to be retained and managed by CSPs, along with the security standards that will have to be applied to keep them safe. Businesses based in the UK and those serving UK customers should not be placed at a commercial disadvantage compared with their overseas competitors.* (Paragraph 71)

10. *Detailed Codes of Practice will be needed to provide a more effective means of assisting compliance, and retaining business confidence in the feasibility of investigatory powers provisions, and their regular updating should be an explicit requirement in the Bill when it is introduced. Specifically, the Bill should require that at regular set intervals (perhaps yearly) the Technical Advisory Board is consulted about keeping the Codes of Practice up to date—a new role we propose for that body—and allowing both the Government and business representatives to bring forward amendments.* (Paragraph 72)

11. From the evidence we have received, it is clear that the Home Office has engaged with communications businesses and the wider internet community. *This should remain a central strand of the Government's strategy to ensure effective implementation and for seeking to allay concerns over current uncertainties and confusion arising from the way some terms are defined in the draft Bill. (We have separately recommended clarifying definitions and strengthening consultation processes through the Technical Advisory Board once the Bill is enacted.)* (Paragraph 75)

12. Internet businesses and their users require assurances that investigatory powers will be imposed proportionately, and that the judgement as to what is proportionate should at all times be open to reasonable challenge. The proposed Investigatory Powers legislation, to the extent that it consolidates and clarifies mostly existing provisions, is itself an important response to that requirement. *The Government should continue to consult and explain fully the likely implications of the proposed legislation.* (Paragraph 76)

13. *The Government should review the composition of the Technical Advisory Board to ensure that it will have members from industry who will be able to give proper consideration, not just to the technical aspects of appeals submitted to it from CSPs concerned about ICR or other interception or 'interference' notices, but also any concerns raised about costs. The Government should also produce an explicit framework for how mediation of disputes and challenge will be resolved. The Government should consider whether the Board will need stronger legal expertise in light of the new investigatory powers that it will have to deal with. Membership of the Board should also more generally reflect a wide range of internet industries and expertise, and be able to co-opt individuals from individual businesses likely to be directly affected.* (Paragraph 80)

14. *The Government did not set up the 'Advisory Council for Digital Technology and Engineering' advocated by the Royal United Services Institute. It should nevertheless add to the remit of the Technical Advisory Board a role it envisaged for that Council—to keep under review the domestic and international implications of the evolution of the internet, digital technology and infrastructure.* (Paragraph 81)

Formal Minutes

Tuesday 19 January 2016

Members present:

Nicola Blackwood, in the Chair

Victoria Borwick	Dr Tania Mathias
Stella Creasy	Derek Thomas
Jim Dowd	Valerie Vaz
Chris Green	Matt Warman

Draft Report (*Investigatory Powers Bill: technology issues*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 84 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Third Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 26 January at 2.00 pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the Committee's inquiry page at www.parliament.uk/science.

Tuesday 10 November 2015

Question number

Matthew Hare, Chief Executive Officer, Gigaclear, **John Shaw**, Vice President, Product Management, Sophos, and **James Blessing**, Chair, Internet Services Providers' Association — Q1–59

Professor Ross Anderson, Professor of Security Engineering, University of Cambridge, **Professor Mike Jackson**, formerly of Birmingham City Business School, **Dr Joss Wright**, Research Fellow, Oxford Internet Institute, and **Professor Sir David Omand GCB**, Visiting Professor, Department of War Studies, King's College London — Q60–90

Tuesday 8 December 2015

Mark Hughes, President, BT Security, and **Antony Walker**, Deputy Chief Executive Officer, techUK — Q91–119

Professor Bernard Silverman, Chief Scientific Adviser, Home Office, **Richard Alcock,** Programme Director of the Communication Capabilities Directorate, Home Office, and **Dr Robert Nowill,** Cyber Security Challenge UK Chairman and Herne Hill Consulting — Q120–167

Published written evidence

The following written evidence was received and can be viewed on the inquiry page of the Committee's website. IPB numbers are generated by the evidence processing system and so may not be complete.

1 Access Now (IPB0049)

2 Adam Langley (IPB0020)

3 Alice Thompson (IPB0022)

4 Andrews & Arnold Ltd (IPB0011)

5 Andy Wootton (IPB0044)

6 Ansgar Koene (IPB0066)

7 Ben Everard (IPB0001)

8 Big Brother Watch (IPB0048)

9 Brass Horn Communications (IPB0019)

10 BT (IPB0061)

11 Christopher Soghoian (IPB0045)

12 Electronic Frontier Foundation (IPB0017)

13 Eric King (IPB0055)

14 Exa Networks Limited (IPB0026)

15 Fellow Claudio Guarnieri (IPB0052)

16 Giuseppe Sollazzo (IPB0024)

17 Graham Smith (IPB0025)

18 GreenNet (IPB0063)

19 Home Office (IPB0030, IPB0065)

20 Information Commissioner's Office (IPB0013)

21 Institute for Human Rights and Business (IHRB) (IPB0035)

22 Internet Infrastructure Coalition (IPB0015)

23 Internet Services Providers' Association (IPB0064)

24 IT-Political Association of Denmark (IPB0051)

25 James Harrison (IPB0059)

26 Jisc (IPB0012)

27 John Phillips (IPB0002)

28 Julian Huppert (IPB0027)

29 Martin Kleppmann (IPB0033)

30 medConfidential (IPB0008)

31 Mozilla (IPB0056)

32 Narration Studio Ltd. (IPB0018)

33 NCC Group plc (IPB0058)

34 New America's Open Technology Institute (IPB0046)

35 Open Rights Group (IPB0034)
36 OpenForum Europe (IPB0047)
37 Philip Virgo (IPB0031)
38 Privacy International (IPB0040)
39 Richard Clayton (IPB0032)
40 Richard Cunningham (IPB0050)
41 Ross Anderson (IPB0036)
42 Software & Information Industry Association (IPB0010)
43 Stanley Shapiro (IPB0057)
44 Timothy Panton (IPB0016)
45 techUK (IPB0037)
46 Universities and Colleges Information Systems Association (UCISA) (IPB0014)
47 William Waites (IPB0005, IPB0021, IPB0028, IPB0029)
48 William Waites/ HUBS C.I.C. (IPB0006)

List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the Committee's website at www.parliament.uk/science.

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2015–16

First Report	The science budget	HC 340 (729)
Second Report	Science in emergencies: UK lessons from Ebola	HC 469
First Special Report	Royal Botanic Gardens, Kew: Government Response to the Committee's Seventh Report of Session 2014–15	HC 454
Second Special Report	Current and future uses of biometric data and technologies: Government Response to the Committee's Sixth Report of Session 2014–15	HC 455
Third Special Report	Advanced genetic techniques for crop improvement: regulation, risk and precaution: Government Response to the Committee's Fifth Report of Session 2014–15	HC 519
Fourth Special Report	The science budget: Government Response to the Committee's First Report of Session 2015–16	HC 729