Internet surveillance

Standard Note: SN/HA/6304
Last updated: 18 May 2012
Author: Philip Ward
Section Home Affairs

In April 2012 reports appeared in the press suggesting that the Government was proposing new legislation to require communication service providers (CSPs) to store all communications data. The intention is to maintain the UK's capability to lawfully intercept and exploit data when fighting crime and terrorism. The Queen's Speech of May 2012 confirmed that a draft Bill is to be introduced. The Government emphasises that the *content* of communications would not be stored, only *communications data* (records of who contacted whom, when, from where, in what technical circumstances and for how long). In the absence of detail, commentators have assumed that this is a reference to the Communications Capabilities Development Programme (CCDP), which already appears in the Home Office Business Plan. The CCDP, in turn, bears similarities to an initiative under the previous Government, the Interception Modernisation Programme.

This note looks at the history of the two programmes, cites the justifications given by successive governments for what critics have dubbed a "snooper's charter" and details some of the objections that have been raised against surveillance of this sort.

Of related interest:

Interception of communications (SN 6332) [summarises powers available under the *Regulation of Investigatory Powers Act 2000* (RIPA)]

Privacy on the internet (SN 5730)

Contents

1 Developments under the Labour Government

1.1 The Interception Modernisation Programme

The interception Modernisation Programme (IMP) was an initiative of the last Government. According to a written parliamentary response of November 2008:

> The objective of the Interception Modernisation Programme (IMP) is to maintain the UK's Lawful Intercept and Communications Data capabilities in the changing communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost. It was established in response to the Prime Minister's National Security remit in 2006...[1]

In February 2008, the then Prime Minister Gordon Brown made a statement to the House on the Chilcot Report and the use of communications intercepts as evidence.[2] This refers to the IMP:

> (...) The Chilcot report also notes that communications technology is changing rapidly; there is a switch towards internet protocol communications, with the clear implications that that brings for our security. Accordingly, we have launched the interception modernisation programme to update our capability to ensure that, under those new circumstances, our national interests will continue to be protected. The new regime for intercept as evidence must be designed to work safely and effectively for that new capability, too...[3]

At this point, the expectation was that there would be a draft bill later in the year. In May 2008, the Government published its draft legislative programme for 2008/09, *Preparing Britain for the future*, which included the following information on a proposed *Communications Data Bill*:

> **The purpose of the Bill is to:** allow communications data capabilities for the prevention and detection of crime and protection of national security to keep up with changing technology through providing for the collection and retention of such data, including data not required for the business purposes of communications service

1 HC Deb 19 November 2008 c593W
2 HC Deb 28 February 2008 c959-71
3 Ibid, c961

providers; and to ensure strict safeguards continue to strike the proper balance between privacy and protecting the public.

The main elements of the Bill are:

- Modify the procedures for acquiring communications data and allow this data to be retained;
- Transpose EU Directive 2006/24/EC on the retention of communications data into UK law.

The main benefits of the Bill are:

- Communications data plays a key role in counter-terrorism investigations, the prevention and detection of crime and protecting the public. The Bill would bring the legislative framework on access to communications data up to date with changes taking place in the telecommunications industry and the move to using Internet Protocol (IP) core networks;
- Unless the legislation is updated to reflect these changes, the ability of authorities to carry out their counter-terror, crime prevention and public safety duties and to counter these threats will be undermined.

Consultation

The Government plans to publish this Bill in draft for pre-legislative scrutiny later this year. The draft Bill will then be made available on www.homeoffice.gov.uk. In the meantime, any comments or questions about these proposals should be directed to CommsData@homeoffice.gsi.gov.uk.

Territorial extent

The Bill would extend to the whole of the United Kingdom. The Government will work closely with the devolved administrations in relation to their responsibilities in this area.[4]

In July 2008, Lord Earl of Northesk asked a number of questions about the programme:

The Earl of Northesk asked Her Majesty's Government:

> *Whether the current Comprehensive Spending Review allocation contains any financing for the Home Office's interception modernisation programme; and, if so, how much*

Lord West of Spithead: As part of the Government's Comprehensive Spending Review (CSR 07) a central bid was made to HM Treasury on behalf of the security and intelligence agencies. Funding for IMP was included in the bid, and the exact programme allocation across the CSR years is currently being finalised between the Home Office and HM Treasury.

The Earl of Northesk asked Her Majesty's Government:

> *What are the Home Office's current budgetary estimates for demonstrating the feasibility of the interception modernisation programme*

---

4 *Preparing Britain for the future*, Cm 7372, May 2008

Lord West of Spithead: A significant proportion of the programme investment over the CSR period will be used to test feasibility and reduce the risk associated with implementing the proposed IMP solution. The private sector is likely to play a major role in this work and the programme will be conducting a competitive tender and entering commercial negotiations to commission its services.

The tendering processes are not yet complete and therefore the budget for the feasibility and de-risking activities is not finalised. For this reason, a precise figure cannot be given at this time.

The Earl of Northesk asked Her Majesty's Government:

> *What are the Home Office's current budgetary estimates for the interception modernisation programme*

Lord West of Spithead: The interception modernisation programme (IMP) will require a substantial level of investment which will need to tie in with the Government's three-year CSR periods. The scale of overall economic investment is very difficult to calculate because of the complexity of the project and wide-ranging implementation solutions currently being considered.

Given this complexity and the commercial and national security sensitivities, the precise costs of the programme cannot be disclosed. Further detail on budgetary estimates for the IMP will, however, become available once the draft Communications Data Bill is published.[5]

In November 2008 Eric Pickles asked about the estimated cost of the programme:

Mr. Pickles: To ask the Secretary of State for the Home Department what estimate she has made of the (a) set-up and (b) annual running costs of the Interception Modernisation Programme database.

Mr. Coaker: The objective of the Interception Modernisation Programme (IMP) is to maintain the UK's Lawful Intercept and Communications Data capabilities in the changing communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost. It was established in response to the Prime Minister's National Security remit in 2006.

As part of the Government's Comprehensive Spending Review (CSR 07) a central bid was made to HM Treasury on behalf of the security and intelligence agencies. Funding for IMP was included in this bid.

The IMP will require a substantial level of investment which will need to tie in with the Government's three-year CSR periods. The scale of overall economic investment is very difficult to calculate because of the complexity of the project and wide ranging implementation solutions currently being considered.

Given the commercial and national security sensitivities, the precise costs of the programme cannot be disclosed. Further detail on budgetary estimates for the IMP will however become available once the public consultation process (announced by the Home Secretary on 15 October) commences in the new year.[6]

---

5 HL Deb 8 July 2008 c75-6WA
6 HC Deb 19 November 2008 c593W

Also in November 2008, in response to another PQ, Home Office Minister Vernon Coaker said:

> We have been considering how we can continue to protect the public by utilising communications data in the light of changing technology and have created the cross-Government Interception Modernisation Programme (IMP) to analyse the available options. Since 2006 there has been ongoing work with intelligence agencies, SOCA, police, HMRC and the telecommunications industry to analyse the size of the problem and to investigate possible solutions to help maintain this essential capability, including relevant safeguards.
>
> I recognise there is a difficult balance between public safety and public rights to privacy so I recently announced my intention to launch a public consultation on the Interception Modernisation Programme. As part of the ongoing engagements with communications service providers, and to raise awareness of the forthcoming consultation, the Interception Modernisation Programme recently presented at the Internet Services Providers' Association conference, outlining the importance of communications data to public safety and the problems that the move to internet technologies will cause. The consultation document also will set out the range of background issues including the vital requirement of communications data in protecting the UK from serious crime and terrorism, the need for a solution to maintain our capability and the need to provide adequate safeguards as part of any solution...[7]

At this stage, although no firm proposals were in the public domain, the press were carrying reports that the data would be stored in a centralised national database. This caused concern in many quarters. The Deputy Information Commissioner was reported as saying, "We have real doubts that such a measure can be justified, or is proportionate or desirable".[8] The BBC reported that the Home Office had been in discussions with mobile phone operators about how to implement a centralised database. On 20 October 2008 the Information Commissioner's Office issued the following statement expressing anxiety about "huge databases":

> This summer the Information Commissioner called for a public debate on government proposals for the state to retain citizens' internet and phone records. The Commissioner warned that it is likely that such a scheme would be a step too far for the British way of life. Creating huge databases containing personal information is never a risk-free option as it is not possible to fully eliminate the danger that the data will fall into the wrong hands. It is therefore of paramount importance that proposals threatening such intrusion into our lives are fully debated. We welcome the fact that the government intends to fully consult the public on any scheme it brings forward. Precise details of the plans are unclear at this stage; the ICO will be studying the proposals once published and responding to the Government's consultation in due course.[9]

For further information on the history of this measure to the end of 2008, see the Library Standard Note, *Draft Communications Data Bill*, (6 January 2009; SN/HA/4884).

---

7 HC Deb 24 November 2008 c830W

8 "Plan to record all calls and emails alarms watchdog", *Guardian*, 21 May 2008

9 Information Commissioner's Office, *ICO Statement on the Communications Data Bill*, 20 October 2008 http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_statement_comms_data_bill.pdf

1.2 The April 2009 consultation

The Queen's Speech 2008 did not include a Communications Data Bill, draft or otherwise. Instead, in a written statement of 27 April 2009, the then Home Secretary, Jacqui Smith, announced a consultation on the collection and use of communications data:

> **The Secretary of State for the Home Department (Jacqui Smith):** I have today published a consultation, "Protecting the Public in a Changing Communications Environment", which addresses the issue of communications data. The consultation explains how existing access to communications data by the police, security and intelligence agencies and by others helps protect and safeguard the public; how the rapidly changing communications environment will make it harder for these agencies and other authorities to obtain access to these data when they need to do so; and the measures we need to take to maintain existing police and agency capabilities in the future. It rules out the option of creating a central database to collect and hold communications data. I am inviting views on the changes we propose and how we will continue to strike the balance between respect for individual privacy and protection of the public.
>
> Communications data are information about a communication not the content of that communication. For a given telephone call, communications data can include the telephone numbers involved, and the time and place the call was made, but not what was said. For an e-mail it might include the e-mail address from which the message was sent, and to where it was sent, but not the content of the message.
>
> Used in the right way, and subject to important safeguards to protect individuals' right to privacy, communications data can play a critical role in keeping all of us safe. It enables investigators to identify suspects and their associates; provides vital clues in solving life-threatening situations such as kidnaps, and evidence supporting alibis and prosecutions; supports lawful interception of communications; and assists the emergency services to help or locate vulnerable people. It is also critical to safeguarding our national security, and in particular to countering the terrorist threat.
>
> Communications data are currently retained by the communications companies for their own business purposes and access by public authorities to any of that data is tightly regulated under the safeguards specified in the Regulation of Investigatory Powers Act 2000, and overseen by the Interception of Communications Commissioner.
>
> The existing regulatory framework which governs access to communications data is based upon the principles of necessity, proportionality, oversight and accountability. Communications data are as vital a tool for investigating and prosecuting crime for our international partners as they are for the UK. Many other countries will face a loss of this capability due to the technological changes in the communications industry. Although other countries will face the same challenges as the UK, we will be among the first to be affected for several reasons:
>
> > The UK telecommunications environment is one of the most dynamic in the world, due to deregulation;
> >
> > Many leading Western European countries still have dominant national fixed line companies, whereas the UK has a more "open" market which encourages the spread and use of communications;
> >
> > The UK's competitive communications market encourages companies to find new ways to cut costs and offer new services, many based in the complex world of the internet.

> Some of these new services will be offered by the companies in the UK that operate the existing communications networks, but many others will be offered by overseas companies outside of UK jurisdiction. They have no need to retain data or provide agencies and the police here with access to it. Consequently, it will become increasingly more difficult to obtain the communications data needed to support public safety. We therefore need to take action to maintain this crucial capability, ensuring that the necessary strict safeguards are retained.
>
> **The consultation rules out creating a central database of communications data.** However, doing nothing in the face of these changes is also not an option. Therefore I am inviting views on other ways in which current capabilities can be maintained in future. Communications companies will continue to be at the heart of the proposed system. They would continue to store data as they do today. But we will need to find ways of collecting and storing data relating to communications services provided from overseas providers.
>
> Any reduction in communications data capabilities will seriously impair the effectiveness of our police and other services to protect the public. Criminals, terrorists and paedophiles are often among early adopters of new technology. We must ensure that our law enforcement agencies can continue to obtain communications data in the face of great technological change.[10] (emphasis added)

The consultation paper is available online.[11] It appears that, if there ever was a plan for a centralised database, it had fallen out of favour by 2009. The emerging preference was for communication service providers (CSPs) to maintain their own databases of collated data, from which authorities could, with proper authorisation, take the information they sought. The paper quoted initial estimates of the implementation costs of the range of options discussed of up "up to £2bn" (p27).

In April 2009, the LSE published a *Briefing on the Interception Modernisation Programme* which contains useful background as well as discussion of the Home Office consultation.[12] The consultation was limited to the handling of what is known as "communications data", essentially records of who contacted whom, when, from where, in what technical circumstances and for how long, but not the *content* of what was said. In response, the LSE's analysis makes the point that, in the fast changing technology of telecommunications, it is becoming increasingly difficult to separate "comms data" from "content":

> We are concerned that the Home Office has not given adequate consideration to the practical and financial challenges of the technologies that would be used to give law enforcement agencies enhanced access to Internet traffic. The "black boxes", as they are known, that would provide ' deep packet inspection' (DPI) facilities would have to collect large amounts of traffic associated with each Internet user, discard whatever appears to be "content" but also to combine different streams of traffic so as to create further information about an individual. (p4)

The Home Office published a summary of responses to the consultation in November 2009. The main themes were set out as follows:

- widespread (but not unanimous) recognition of the importance of communications data in protecting the public

---

10 HC Deb 27 April 2009 c36-7WS

11 *Protecting the public in a changing communications environment*, Cm 7586, April 2009

12 http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

- widespread appreciation of the challenges which rapidly changing technology poses
- some support for the Government's proposed ways of meeting these challenges
- but also concerns about whether the Government's proposals would be technically feasible or would impose unreasonable burdens on industry
- some concern about whether the assessment of the balance of costs and benefits of the Government's proposals was realistic
- a desire from a number of respondents for greater clarity on why existing legislation and regulations were not capable of meeting the Government's stated requirements
- but also a recognition, particularly amongst those involved in the communications industry, that current legislation and regulations relating to the collection, retention and processing of communications data, particularly third party data, would soon need to be updated in light of changing technology
- concerns about protecting communications data, where both privacy and commercial interests were engaged
- calls for more judicial involvement, and greater visibility and public awareness of existing oversight mechanisms, in order to improve public confidence in the way public authorities use communications data to protect them.[13]

In December 2009 Baroness Miller of Chilthorne Domer asked about the timetable for taking forward the IMP:

> Asked by **Baroness Miller of Chilthorne Domer**
>
> > To ask Her Majesty's Government what is their timetable for taking forward the Interception Modernisation Programme and the Mastering the Internet programme.
>
> **The Parliamentary Under-Secretary of State, Home Office** (Lord West of Spithead): As a result of this year's communications data consultation the Government will continue to develop their proposed approach. This approach will require legislation to ensure that the data required by public authorities to protect the public are collected and retained by communications service providers. **Plans for legislation are not developed sufficiently for it to be included in this Session of Parliament**.
>
> Separately, as outlined in its public statement on 3 May 2009, GCHQ has an ongoing programme of investment in the technology and skills needed to keep one step ahead of the threats facing the UK.[14] (emphasis added)

And in January 2010 Chris Huhne asked:

> **Chris Huhne**: To ask the Secretary of State for the Home Department what assessment he has made of the compatibility of (a) his Department's programme of intercepting communications data and (b) the proposed Interception Modernisation

---

13 *Summary of Responses to the 2009 Consultation Paper*, p4

14 HL Deb 10 December 2009 c159-60WA

> Programme with the requirements of the Data Retention (EC Directive) Regulations 2009.
>
> **Alan Johnson**: The Data Retention (EC Directive) Regulations 2009 completed the transposition of Directive 2006/24/EC on the retention of communications data. Since 2005, when the directive was negotiated, there has been continuous and innovative development of communications services and applications, many of which are not covered by current data retention legislation. This has already started to undermine the capabilities of our law enforcement and national security agencies to protect the public.
>
> Last year a public consultation, "Protecting the public in a changing communications environment", sought views on proposals to maintain investigative capabilities in the face of these challenges. In response to that consultation the Government are developing its proposed approach, continuing to work closely with communications service providers to minimise as far as possible any impact on them, and ensuring that any new proposals include strong safeguards to minimise the potential for abuse, and to maintain the security and integrity of the data.[15]

1.3 The EC Directive on Data Retention

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

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

However, it has been suggested, the Directive does not include some of the data that IMP (or successor proposals) would propose collecting, in particular data like that generated through the use of VoIP (voice over IP), instant messaging and social networking websites.[16] The IMP, as described in draft form in the Home Office consultation document, promised to go beyond the Directive by requiring the storage of third-party data:

> Communications service providers based in the UK would […] continue to collect and retain communications data relating to their own services but **also collect and store the additional third party data crossing their networks**. This would therefore include communications data which does not come under the scope of the EU Data

---

15 HC Deb 28 January 2010 c1048W

16 According to a "wiki" analysis on the website of the Open Rights Group

> Retention Directive […]. This option would resolve the problem that some communications data which may be important to public authorities will not otherwise be retained in this country. However, it would not address the problem of fragmentation: as data is increasingly held by a wider range of communications service providers, it might take longer than it does at present to piece together data from different companies relating to one person or communications device. The current capability would therefore diminish […].To mitigate this problem the Government would require communications service providers not only to collect and store data but to organise it, matching third party data to their own data where it had features in common (for example, where it relates to the same person or to the same communications device). This would require additional legislation.[17] (emphasis added)

2 Developments under the Coalition

The Coalition Agreement included an undertaking to "end the storage of internet and email records without good reason".[18] In the 18 May 2010 issue of *Computer Weekly* this was interpreted as a threat to the programme's future:

> The parties also agreed to end "storage of internet and e-mail records without good reason". This appeared to put at risk the £12bn Interception Modernisation Programme which would have collected and stored every message sent and received by the UK's networks.
>
> However, internet service providers already collect address and time details of e-mails and voice calls made over the internet under the European Data Retention Directive and the Regulation of Investigatory Powers Act (Ripa).

On 20 May 2010, the *Financial Times* reported a speech by the Deputy Prime Minister:

> The Liberal Democrat leader is in charge of what he calls "the biggest shake-up of our democracy" for more than 150 years, setting out an agenda spanning House of Lords and electoral reform and plans to curb "the surveillance state". His promise not to store internet and e-mail records suggested the new government has plans to scrap the £2bn Home Office "intercept modernisation programme", which aims to bring wire-tapping into the internet age.
>
> However, Home Office officials were at pains yesterday to point out the debate on the project's survival was still "very much on". The country's most senior police officers and the security services have said it will be impossible to do their jobs without having the ability to track internet traffic.
>
> Talks between the government and senior MI5 and Scotland Yard officials are expected to go on for a week, with a resolution expected before next week's Queen's Speech.[19]

Subsequently, the Queen's Speech on 25 May announced a forthcoming *Freedom (Great Repeal) Bill*. Some possible measures of likely impact on the Interception Modernisation Programme (IMP) were alluded to:

> The main benefits of the Bill would be:
>
> The exact content of the Bill will be announced in due course and could cover a range of benefits, including:

---

17 *Protecting the public in a changing communications environment*, Cm 7586, April 2009, para 3.2
18 HM Government, *The Coalition: our programme for government*, May 2010, p11
19 "Clegg to roll back 'Big Brother state'", *Financial Times*, 20 May 2010

> [...]
>
> Ensuring the storage of internet and email records is only done when there is good reason to do so.
>
> The main elements of the Bill are:
>
> The exact content of the Bill will be announced in due course and could cover a range of policies, including:
>
> [..]
>
> Ending of storage of internet and email records without good reason

However, the resultant *Protection of Freedoms Bill* (which is currently in its final parliamentary stages) does not contain any measures about data retention.[20] It seems that legislation in this area is still under consideration.

2.1 The Communications Capabilities Development Programme

One section of the Strategic Defence and Security Review published in October 2010 speaks of the "need to adapt our strategy for countering international terrorism". The review then sets out proposals for achieving that end. This is one of them:

> We will... introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communication data and to intercept communications within the appropriate legal framework. This programme is required to keep up with changing technology and to maintain capabilities that are vital to the work these agencies do to protect the public. Communications data provides evidence in court to secure convictions of those engaged in activities that cause serious harm. It has played a role in every major Security Service counterterrorism operation and in 95% of all serious organised crime investigations. We will legislate to put in place the necessary regulations and safeguards to ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties.[21]

A number of commentators read this as a "revival" of the previous Government's plans for IMP, now apparently renamed the "Communications Capabilities Development Programme".[22] Tom Watson tabled an Early Day Motion to that effect:

> That this House expresses its deep concern about the Government's proposal, contained within the Strategic Defence and Security Review, to develop an interception modernisation programme; notes that such a programme would include a proposal to store every email, webpage visit and telephone call made in the UK for an unspecified period; further notes that the Home Office has previously estimated that such a database would cost in the region of 2 billion to develop; believes that the development of an interception modernisation programme raises serious privacy, data storage and access concerns; and calls on the Government to issue a full public consultation on its proposals as soon as possible.[23]

---

20 There are clauses amending the *Regulation of Investigatory Powers Act 2000*, but this is in relation to *access* to data and judicial oversight. See the Library Research Paper on the Bill.

21 Ministry of Defence, *Securing Britain in an age of uncertainty: Strategic Defence and Security Review*, October 2010, pp43-4

22 E.g. "Plan to store Britons' phone and internet data revived", *Guardian*, 20 October 2010

23 Interception modernisation programme, EDM 1247 2010-12, 11 January 2011 (22 signatures to date).

The Counter-Terrorism Strategy, published in July 2011, confirms the Government's intention to bring forward legislation to regulate the ability of the security services and the police to access such communications data and track the use of mobiles, email and other data transfers:

> 4.40 Communications data is an important tool for investigators and provides an invaluable means by which the police and law enforcement agencies can better safeguard the public. But our current capability was not designed to deal with the growth in the use of internet-based communications. The ability of the security, intelligence and law enforcement agencies to use internet-based communications data will decline unless action is taken. As we set out in the Strategic Defence and Security Review (SDSR) the Government will therefore introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communications data and also to intercept communications within the appropriate legal framework. Legislation will be brought forward to put in place the necessary regulations and safeguards to ensure that the response to this technology challenge is compatible with the Government's approach to information storage and civil liberties.[24]

The Home Office *Business Plan 2011-15* contains this timetable for future action:

> **5.3 End the storage of internet and email records without good reason**
>
> i. Develop and publish proposals for the storage and acquisition of internet and email records [started – end April 2012]
>
> ii. Implement key proposals for the storage and acquisition of internet and email records, including introducing legislation as necessary [started – June 2015][25]

The Home Office *Business Plan* replaces the draft Structural Reform Plan published in July 2010. Since that date the Department has been publishing monthly "implementation updates" to the Structural Reform Plan. According to the latest of these, dated March 2012, "work [is] ongoing" on the two actions announced in paragraph 5.3.

The Home Office webpage on "Communications data" includes this statement about the Communications Capabilities Development programme:

> The... programme was set up to look at how we can preserve communications capabilities to protect the public in the future, as internet-based communications technology becomes increasingly popular.
>
> We are already addressing some of the challenges posed by changing communications services by improving the training of investigators and by improving the efficiency and safeguards for acquiring communications data; however we need to do more.
>
> Our work is about maintaining existing capabilities and established and effective ways of tackling serious crime and countering terrorism. It is not about developing new, more intrusive powers.
>
> When legislating, which we have committed to do in the SDSR, striking the balance between the right to privacy and the right to safety will both be paramount. The ongoing use of current communications data capabilities will be focused and

---

[24] *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, Cm 8123, July 2011, p53

[25] Home Office, *Business Plan 2011-15*, May 2011

> proportionate with strict safeguards in place to prevent any abuse of data. Details of this legislation will be announced in Parliament in due course.

These are the most recent parliamentary answers on the current programme:

> **Mr Raab:** To ask the Secretary of State for the Home Department when she plans to bring forward legislative proposals for the Intercept Modernisation programme. [94397]
>
> **James Brokenshire** *[holding answer 9 February 2012]:* The Interception Modernisation programme was a programme set up under the previous Government which has been superseded by the policies of the coalition Government. As we made clear in the strategic defence and security review the Government will continue to work to preserve the ability of the law enforcement, security and intelligence agencies to obtain communications data and to intercept communications within an appropriate legal framework. Through the Communications Capabilities Development programme we will ensure this is compatible with the Government's approach to civil liberties. As set out in the Home Office's Structural Reform Plan, details of this legislation will be announced in Parliament in due course.[26]
>
> **Mr David Davis:** To ask the Secretary of State for the Home Department whether the Internet Service Providers' Association has been included in consultation on the Communications Capabilities Development programme; and what steps have been taken to include all internet service providers in such discussions. [98431]
>
> **James Brokenshire** *[holding answer 6 March 2012]:* Home Office officials have met with the main industry associations representing internet service providers and communications service providers to discuss the cross-Government Communication Capabilities Development programme. These meetings have included the Internet Service Providers' Association whose advice has been sought on how and when to engage with all interested internet service providers, as part of the Department's ongoing engagement strategy with industry.[27]

2.2 The news stories of April 2012

In April 2012, in a front-page story, the *Sunday Times* reported further details of the proposals. According to the report, internet companies would be told to install hardware to allow GCHQ to scrutinise "on demand" every phone call made, text message and email sent and website accessed in real time. MI5 and GCHQ, it is asserted, have lobbied for such powers, which they believe are a crucial tool to combat terrorism and serious crime:

> While the new law would not allow GCHQ to monitor the content of communications without obtaining a warrant, it would permit the intelligence agency to trace whom a person or group had contacted, when, for how long and for how often.[28]

The story was picked up elsewhere in the media. A long follow-up article in the *Sunday Times* the following week highlighted some of the technical challenges involved in introducing such technology. For example, to capture traffic on services such as Skype, which is encrypted, the black boxes would have to use "deep packet inspection" to decode who is in contact with whom. To break this, and the encryption method used by Gmail and others known as "https", would take "significant resources" as well as "jeopardising" the e-commerce industry.[29] One major UK internet service provider told the BBC there was a risk

---

26 HC Deb 20 February 2012 c505W
27 HC Deb 8 March 2012 c841W
28 "Government to snoop on all emails", *Sunday Times*, 1 April 2012, p1
29 "Every click you make, every call you take, they'll be watching you", *Sunday Times*, 8 April 2012, p18

that data could be fragmented as different companies use various methods and third-parties to handle the vast amounts of information.[30] The Equality and Human Rights Commission has stated that the plans "would potentially be incompatible with the right to privacy of many ordinary people in the UK."[31] Specifically, it is suggested that the proposals might breach the European Convention on Human Rights, which gives an individual a right to privacy (under Article 8).[32]

In justification of the proposals, the Home Secretary and Justice Secretary sent a letter to all Conservative MPs explaining that law enforcers had to keep one step ahead:

> Communications data – information such as who called whom and at what time – is vital to law enforcement, especially when dealing with organised crime gangs, paedophile rings and terrorist groups. It has played a role in every major Security Service counter-terrorism operation and in 95 per cent of all serious organised crime investigations. Communications data can and is regularly used by the Crown Prosecution Service as evidence in court.
>
> But communications technology is changing fast, and criminals and terrorists are increasingly moving away from landline and mobile telephones to communications on the internet, including voice over internet services, like Skype, and instant messaging services. Data from these technologies is not as accessible as data from older communications systems which means the police and Security Service are finding it increasingly hard to investigate very serious criminality and terrorism. We estimate that we are now only able to access some 75% of the total communications data generated in this country, compared with 90% in 2006. Given the pace of technological change, the rate of degradation could increase, making our future capability very uncertain.[33]

David Davis, a former Shadow Home Secretary, opposes the plans:

> "What this does is make (existing problems) 60 million times worse. The simple truth is that this is not necessary. What's proposed here is completely unfettered access to every single communication you make.
>
> "It's a very, very big widening of powers which will be very much resented by many citizens who do not like the idea. It's going to cause enormous resentment."[34]

In an article in *The Sun*, the opposing views of Mrs May and Mr Davis were published, under the title "Are GCHQ set to spy on you?"[35] The press has also suggested that there is a difference of opinion about the proposals between Conservative and Liberal Democrat members of the Coalition.[36] The Deputy Prime Minister has promised an "open... and properly scrutinised consultation" on the proposals.[37]

The Government stresses that what is proposed is merely an expansion of existing powers, which cover more traditional forms of communication, to new technology. The authorities

---

30 "Analysis: will the government's web 'snoop' plans work?", *BBC News*, 2 April 2012

31 EHRC, "Commission's statement on privacy", 3 April 2012

32 "New snooping powers could be illegal, human rights watchdog warns," *Daily Telegraph*, 4 April 2012

33 Quoted on the Conservative Home blog, 5 April 2012; "Theresa May and Kenneth Clarke urge Tories to back security plan", *Guardian*, 5 April 2012

34 Quoted in "New powers to record every phone call and email makes surveillance '60m times worse'", *Daily Telegraph*, 2 April 2012

35 "Terrorism Debate", *The Sun*, 3 April 2012

36 "Cameron and Clegg clash over secret courts and email monitoring", *Guardian*, 10 April 2012

37 "Data privacy: Clegg attempts to quell criticism", *Financial Times*, 4 April 2012, p4

would still need a warrant to access the contents of such communication.[38] Officials also underline a difference between the current proposals and the early proposals for an Intercept Modernisation Programme (IMP) initiated under the previous Government. The IMP – *in the proposals as originally reported in 2008* -- would have compelled internet service providers and phone companies to gather customer data, to be fed into a centralised database.[39] The current scheme does not involve a centralised system, but focuses only on web and social media providers storing information that can be accessed by police and security services on demand.[40]

According to the press, draft clauses of a future Bill were expected to be published around the time of the Queen's speech in May 2012. It was reported that a select committee would hold "public hearings to subject them to 'proper, pre-legislative scrutiny'".[41]

2.3 The Queen's Speech 2012

A draft Communications Data Bill was announced in the Queen's Speech. The Cabinet Office has produced a short briefing note on what is planned:

> **Draft Communications Data Bill**
>
> "My Government intends to bring forward measures to maintain the ability of the law enforcement and intelligence agencies to access vital communications data under strict safeguards to protect the public, subject to scrutiny of draft clauses."
>
> **The purpose of the draft Bill is to:**
>
> - The draft Bill would protect the public by ensuring that law enforcement agencies and others continue to have access to communications data so that they can bring offenders to justice.
>
> **What is communications data:**
>
> - Communications data is information about a communication, not the communication itself. Communication data is NOT the content of any communication - the text of an email, or conversation on a telephone.
>
> - Communications data includes the time and duration of the communication, the telephone number or email address which has been contacted and sometimes the location of the originator of the communication.
>
> **The main benefits of the draft Bill would be:**
>
> - The ability of the police and intelligence agencies to continue to access communications data which is vital in supporting their work in protecting the public.
>
> - An updated framework for the collection, retention and acquisition of communications data which enables a flexible response to technological change.
>
> **The main elements of the draft Bill are:**

---

38 "Senior Lib Dem threatens to block surveillance plans", *Guardian*, 8 April 2012

39 Note, however, that by 2009 the previous Government had ruled out a "Big Brother" database in favour of localised data retention by CSPs.

40 "Q&A The proposals: increased powers prompt fears over costs and 'big brother' state", *Financial Times*, 4 April 2012, p4

41 "Every click you make, every call you take, they'll be watching you", *Sunday Times*, 8 April 2012, p18

- Establishing an updated framework for the collection and retention of communications data by communication service providers (CSPs) to ensure communications data remains available to law enforcement and other authorised public authorities.

- Establishing an updated framework to facilitate the lawful, efficient and effective obtaining of communications data by authorised public authorities including law enforcement and intelligence agencies.

- Establishing strict safeguards including: a 12 month limit of the length of time for which communications data may be retained by CSPs and measures to protect the data from unauthorised access or disclosure. (It will continue to be the role of the Information Commissioner to keep under review the operation of the provisions relating to the security of retained communications data and their destruction at the end of the 12 month retention period)

- Providing for appropriate independent oversight including: extending the role of the Interception of Communications Commissioner to oversee the collection of communications data by communications service providers; providing a communications service provider with the ability to consult an independent Government / Industry body (the Technical Advisory Board) to consider the impact of obligations placed upon them; extending the role of the independent Investigatory Powers Tribunal (made up of senior judicial figures) to ensure that individuals have a proper avenue of complaint and independent investigation if they think the powers have been used unlawfully.

- Removing other statutory powers with weaker safeguards to acquire communications data.

Existing legislation in this area is:

- Regulation of Investigatory Powers Act 2000

- The Data Retention (EC Directive) Regulations 2009

Devolution:

The Bill would apply to England, Wales, Scotland and Northern Ireland and relates to non-transferred matters.[42]

[42] Cabinet Office, *The Queen's Speech 2012 - Briefing Notes*, 9 May 2012, p44-45