Liberty’s Submission to the Joint Committee on the Draft Communications Data Bill

August 2012
About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK’s leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty’s policy papers are available at

Contact

Isabella Sankey
Director of Policy
Direct Line 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sophie Farthing
Policy Officer
Direct Line 020 7378 3654
Email: Sophief@liberty-human-rights.org.uk
‘Today we are in danger of living in a control state. Every month over 1,000 surveillance operations are carried out. The tentacles of the state can even rifle through your bins for juicy information.’

The Rt Hon David Cameron MP, June 2009
Executive Summary

The Draft Communications Data Bill relates to the proposed collection, retention and availability of “communications data” across the UK. It is no exaggeration to say that these legislative proposals signal a major shift in the relationship between the communications industry, the state and the public. Never before have private companies been called upon to orchestrate blanket collection of personal data which they have no business reason to retain. This briefing will interrogate the capacity which could be created under these proposals, the depth of the civil liberties implications and the limitations of the proposed system in law enforcement terms.

Communications data is highly revealing. In an average day we can expect to generate a large amount of communications data, including from activity on social networking sites such as Facebook and LinkedIn, the details of communications via Twitter, the history of websites visited, the time at which telephone calls were made, who they were made to and how long the call lasted, the location of an individual making or receiving a mobile phone call as well as the duration and timing of the phone call and subscriber information relating to the source or recipient of communications and their direct debit details.

Such data is increasingly difficult to distinguish from “content” and we understand that in order to facilitate the collection of data under this Bill, telecommunication providers will be required to install technology that has the capacity to routinely intercept all communications. This not only exacerbates human rights concerns but also makes clear that this proposal is about extending rather than maintaining the ability of the State to monitor communications.

In the UK arrangements currently exist for the retention of some communications data. This is as a result of an EU Directive that was transposed into UK law in 2009. However, similar rules in place in other EU countries have been recently subject to successful legal challenge. Indeed constitutional courts across the continent – including in Germany, Romania and Bulgaria – have ruled that their respective arrangements for retaining some communications data are unconstitutional. A significant case is currently pending before the European Court of Justice which, for the first time, will directly interrogate the compatibility of the EU Directive with human rights obligations. We are unsure why the Government has not waited for the outcome of this judgment before pressing ahead with more intrusive plans.
Liberty believes that current UK data retention arrangements are a disproportionate interference with the right to respect for private life and undermine respect for freedom of expression. The proposals set out in the Draft Bill go significantly further and suffer even greater flaws as a result.

Liberty has never opposed targeted surveillance with prior authorisation, on the basis of individual suspicion, but this Draft Bill amounts to nothing less than blanket surveillance of the population at large, turning a nation of citizens into a nation of suspects.
Introduction

1. The Draft Communications Data Bill (‘the Draft Bill’) was announced in the Queen’s Speech and published by the Home Office on 14\textsuperscript{th} June 2012. It is currently undergoing a period of pre-legislative scrutiny by the Draft Communications Data Bill Committee (‘the Committee’). Liberty appreciates the opportunity presented by pre-legislative scrutiny of the Draft Bill, but given the privacy implications these proposals carry for all UK residents we are disappointed that there has been no prior public consultation undertaken by the responsible department. In particular, we understand that there has been no formal process of consultation with communication service providers. On this basis we find it very difficult to understand how the Home Office has reached its conclusions about the extent of potential collaboration, nor indeed the costs implications of its proposals.

2. Before embarking on a substantial analysis of these proposals we must further express concern at their broad and vague nature. Our attempts to critique this Draft Bill have been hampered by a serious lack of detail. The best way to describe its provisions is ‘future-proof’: highly enabling and lacking in focused prescription.

The detail of the Draft Bill

Part 1 - Data Collection

3. Clause 1 of the Draft Bill grants the Secretary of State the power, by order, to impose any requirement or restriction on an operator which is aimed at ensuring the availability of communications data to specified bodies. Arrangements around access to data are dealt with in Part 2, but Clause 1(b) makes clear that operators may be required to retain or otherwise handle data in order to facilitate access outside the arrangements provided for in Part 2 of the Draft Bill. The non-exhaustive list of requirements which may be imposed on operators include obtaining or processing data and entering arrangements with third parties in order to facilitate the availability of data.\textsuperscript{1} The processing of data includes the reading, organisation, analysis, copying, correction, adaptation or retrieval of data and its integration with other data.\textsuperscript{2}

\begin{table}
\begin{tabular}{|c|c|}
\hline
1 & Clause 1(2).
\hline
2 & Clause 1(5).
\hline
\end{tabular}
\end{table}
Requirements may be placed directly on an operator by order or provision may be made in an order to allow for restrictions or requirements to be imposed by notice.\(^3\)

4. Subclause 1(3) provides that operators may be made subject to additional regulatory obligations designed to facilitate swift access to data and make provision about standards, equipment, systems and techniques.\(^4\) Requirements may be placed on operators in relation to services provided by another operator. Communications data for the purposes of the permissive regime set up by clause 1 carries substantially the same meaning as provided for under RIPA; the regime applies to postal operators.\(^5\) Subclause 1(4) states that an authorisation may not permit conduct consisting of the interception of communications; as explored below this prohibition is difficult to square with our knowledge of the technological limitations of DPI software and hardware.

5. Under the heading ‘safeguards’ clause 2 places the Secretary of State under an obligation to consult with OFCOM, the Technical Advisory Board and operators or persons representing operators or with statutory functions in relation to operators.\(^6\) The Technical Advisory Board is solely concerned with the technical or financial viability and not the privacy impact of proposals.

6. Clause 4 provides that data must be retained for 12 months from the date of the communication unless a shorter period is provided for in a specific notice or the operator is informed that the data is or may be required for legal proceedings, in which case operators will be required to retain data until informed otherwise. If it becomes apparent that communications data is not required for legal proceedings, the public authority which has requested the information should inform the operator of that fact.

7. Clause 5 makes clear that operators cannot disclose data except in accordance with Part 2 of the Draft Bill dealing with access and authorisation, or ‘otherwise as authorised by law’; this could include a disclosure required by court order as suggested by the explanatory memorandum, but would clearly cover other situations in which the Secretary of State authorises access otherwise than in

---

\(^3\) Clause 1(2)(b).
\(^4\) Clause 1(3).
\(^5\) Clauses 28 and 25.
\(^6\) Clause 2.
accordance with Part 2 under subclause 1(b). The operator is required to put in place security provision to protect against unlawful disclosure which can include management checks and controls; no further detail is provided about the requirement of ‘adequate security systems’.  

8. Clause 6 provides for the destruction of data at the end of the retention period. Destruction can take place at monthly intervals, meaning data can be retained for up to an additional month pending the next round of data destruction.

9. Clause 7 sets out ‘other safeguards’. All listed safeguards set out in this section of the Bill relate to process and specifically the form of requests. A notice made pursuant to an order requiring retention of data must be in writing, specify the recipient and be given in a manner ‘appropriate’ to bring it to the intention of the recipient.  

10. Clause 8 deals with enforcement. Requirements dealing with the way data should be held, the duration of retention, access and destruction or any other requirement or restriction imposed by order are enforceable by the Secretary of State through civil proceedings. Where work is incidental to or ‘reasonably undertaken in connection with’ conduct that is authorised under this Part of the Bill and it is not conduct for which an authorisation or warrant could and should have been sought independently, it is not to lead to civil liability.

Part 2 - Accessing data

11. Clause 9 makes legislative provision, via a process of internal authorisation, for access to all forms of communications data by any police force, the Serious

---

7 Clause 5(2).
8 Clause 7(1).
9 Clause 8(3).
10 Clause 8(4).
Organised Crime Agency, HMRC, the intelligence services and any other public authority designated in a Secretary of State order.\textsuperscript{11} Before data can be accessed by an employee the authorisation of a designated senior officer of the authority concerned must be sought. If granted the employee who made the request becomes an authorised officer for the purposes of the request. The designated senior officer may only grant authorisations where he or she believes that it is:

(i) necessary to acquire the data for a permitted purpose;
(ii) necessary to obtain the data:
   (a) for the purposes of a specific investigation or operation; or
   (b) ‘for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data’; and
(iii) the conduct authorised is necessary and proportionate to the aim.\textsuperscript{12}

12. This provision mirrors RIPA and the permitted purposes set out at subclause 9(6) remain as broad and ill-defined. An additional purpose is added at subclause 6(c) which relates to the prevention and detection of any conduct in respect of which civil enforcement action for market abuse may be taken by the Financial Services Authority.\textsuperscript{13} These permitted purposes can be added to or restricted by the Secretary of State by order.\textsuperscript{14}

13. The designated senior officer may grant authorisation for himself or any other employee within his public authority and the authorisation can extend to any conduct in relation to a communications system or data derived from such a system in order to obtain communications data.\textsuperscript{15} Clause 9(3) contains a non-exhaustive list of the type of conduct which can be authorised including requiring any person whom the authorised officer believes holds communications data to disclose it to a person identified in the authorisation. Clause 9(4) states that an authorisation may grant access to communications data to a person who is not authorised in the order for any conduct which has, as its aim, the enabling or facilitating of obtaining communications data. Subclause 9(5)(b) provides that authorisations made under

\textsuperscript{11} Clause 21.
\textsuperscript{12} Clause 9(1).
\textsuperscript{13} The Draft Bill provides for the repeal of other corresponding powers and is therefore effectively a consolidation of existing provision in one piece of legislation.
\textsuperscript{14} Clause 9(7).
\textsuperscript{15} Clause 9(2).
sub-clause 9(3) may not involve the disclosure of data to those outside of the public authority in question.

14. Clause 10 makes provision for the form in which authorisations or notices made pursuant to authorisations are to be made – in particular the nature of requirements should be specified. Notices must specify the office or position of the person giving it, the requirements imposed and the operator upon whom the requirements are imposed.

15. Clause 11 sets out a regime of judicial approval for local authority access to communications data which mirrors the provisions of sections 23A and B of RIPA. Where an application is made for a Magistrate’s order approving an authorisation, the individual who is the subject of the authorisation need not be informed; the same is true of his legal representatives. A Magistrate may approve the authorisation where satisfied that, at the time of the grant and at the time the application comes before the Court, the requirements set out at subclause 9(1), which deal with internal authorisation, are satisfied.

16. Local authorities can still only seek access to use and subscriber data. Aside from local authorities and those public authorities listed on the face of the Draft Bill, provision around the range of public authorities to which access will be granted, the types of data to which access is authorised and authorisation processes are left to secondary legislation: no draft order has yet been forthcoming.

17. Clause 12 provides for authorisations to be operational for renewable periods of a month. If the grounds for the original authorisation no longer exist, a designated senior officer must cancel the authorisation. Clause 13 places operators under a duty (enforceable by civil proceedings brought by the Secretary of State) to ‘obtain or disclose the communications data in a way that minimises the amount of data that needs to be processed for the purpose concerned’. Clause 13 also reaffirms an operator’s duty to act in accordance with the requirements of a notice given in accordance with an authorisation, however they are not required to do anything in pursuance of that duty which it is not reasonably practicable to expect them to do.

---

16 Uncommenced provisions inserted by section 37 of the Protection of Freedoms Act 2012.
17 See clause 17.
18 We understand that the Secretary of State has asked those public authorities seeking to retain access to communications data to set out the ‘business case’ for ongoing access.
19 Clause 13(1).
18. Clause 14 provides for filtering arrangements to be put in place by Government. The clause is incredibly broadly framed and its scope obscure. The Secretary of State is empowered to put in place any ‘arrangements’ she sees fit, for the purposes of ‘assisting’ operators to determine whether retention could be secured in accordance with the provisions of clause 9, or to ‘facilitate’ efficient and effective access to data. In particular the Secretary of State can obtain data on behalf of an authorised officer and obtain the ‘data from which the data may be derived’. It is also clear that the Secretary of State can retain data for the purpose of processing that data, allowing for temporary executive retention, processing and distribution of data brought together from many different sources. The Government maintains that clause 14 is designed to create an automated system which will ensure that only that information relevant and required by a particular authorisation is retained, but the extent to which this central filter will be automated is not clear. Clause 16 which sets out duties in connection with the operation of the filter provides that aside from disclosure to designated senior officers, disclosure is permitted for the purposes of support, maintenance, oversight, operation or administration of the filtering arrangements. What is clear is that the filter amounts to a temporary centralised store of potentially large amounts of communications data operated and maintained by the executive, giving the Government a very significant role at the centre of the data retention and disclosure regime.

19. Through the filter, the Secretary of State will seek to make public authorities aware of the extent of communications data available and process data with disclosure based on an assessment of what is needed by the requesting authority. The central filter will bring together atomised pieces of data to create a revealing whole. Further, according to Professor Peter Sommer, a leading technical expert in the field, the filter is likely to use ‘content’ and ‘communications data’ in order to correctly identify patterns of communication.

20 Clause 14(2)(b).
21 Clause 14(2). In the accompanying explanatory notes the Government notes that data generated by current forms of online communication will require greater aggregation and processing – for example they envisage cases in which fragmented communications data from a number of different sources will be co-ordinated through the filter to provide a fuller picture.
22 Submission of Professor Peter Sommer to the Joint Committee on the Draft Communications Bill, para 44.
20. Clause 15 makes clear that the proposed central filter may be used both for the purposes of obtaining and disclosing communications data. Subclause 15(2) refers to the temporary retention of data and subclause 16(1)(c) provides for the destruction of data obtained and processed through the filter ‘when the purposes of the authorisation have been met’: no upper time limit for retention of data in the central filter is provided. An authorisation made by a designated senior officer must record the officer’s decision as to whether data is to be obtained and disclosed through this centralised process and the description of data that may be processed in accordance with a particular authorisation. Clause 16 restates the purposes for which communications data retained in the central store can be disclosed. There is a requirement to put in place a security system to govern access, no details are given about the form or extent of security required. Retrospective annual reports on the operation of the filtering database are to be supplied by the Secretary of State to the Interception of Communications Commissioner as soon as possible after the end of each calendar year.\textsuperscript{23} ‘Significant processing errors’ must be reported to the Commissioner.\textsuperscript{24}

21. Clause 17 provides that local authorities may not access traffic data or any extra data ‘generated’ by operators in response to a request by a relevant public authority. The Secretary of State may place restrictions on the granting of authorisations by designated senior officers including in relation to data stored by Government as part of ‘filtering arrangements’.\textsuperscript{25} The Secretary of State may delegate any of her functions in relation to filtering arrangements to a designated public authority.

\textit{Part 3 - Scrutiny of retention of and access to communications data}

22. Part 3 replicates provisions of RIPA providing for the retrospective oversight of data retention and disclosure by the Interception of Communications Commissioner.\textsuperscript{26} Operators must keep sufficient records of actions taken in accordance with the provisions of the Bill to allow for review by the Commissioner.\textsuperscript{27}

\begin{itemize}
\item\textsuperscript{23} Clause 16(6).
\item\textsuperscript{24} Clause 16(7).
\item\textsuperscript{25} Clause 17(4).
\item\textsuperscript{26} Save where oversight is reserved to the Information Commissioner or the judiciary (under clause 22(1), this is a Magistrate for England and Wales).
\item\textsuperscript{27} Clause 22(6).
\end{itemize}
23. Clause 23 provides for the jurisdiction of the Investigatory Powers Tribunal to be extended to cover new powers granted under Parts 1 and 2.

Part 3 – general provisions

24. Clause 25 extends the reach of Parts 1 and 2 to cover postal operators in the same way as they apply to telecommunications operators. Clause 26 obliges the Secretary of State to make payments towards the costs incurred or likely to be incurred by telecommunications and postal operators. Payment may be made subject to conditions. It is for the Secretary of State to determine the scope and extent of arrangements for payments, including specifying which payments should be made to particular operators. Clause 27 incorporates Schedule 3 which provides for amendments to RIPA to extend Codes of Practice to cover the provisions of this Draft Bill. Schedule 3 also provides for amendments to RIPA allowing for regular revision of codes of practice. The Secretary of State is required to consider representations made around draft codes and may modify a draft. Both codes and revisions to codes must be laid before Parliament and are subject to the affirmative resolution procedure.

Background

25. The Regulation of Investigatory Powers Act 2000 (RIPA) governs the use of targeted surveillance in the UK. Before RIPA came into force, our statute book contained a number of targeted surveillance powers developed in an ad hoc way over the years. RIPA was designed to consolidate the law and to incorporate human rights principles of necessity and proportionality. At its inception, RIPA was designed to deal with access to communications data and access is currently governed by Chapter I, Part II of RIPA and the Regulation of Investigatory Powers (Communications Data) Order 2010. Section 22(4) of RIPA provides the current definition of communications data which has three components:

(i) Traffic data: this tells you, amongst other things, where the mobile phone, internet connection etc was located at the time a communication took place – e.g. where a mobile phone was when it received or made a call as well as data going to the identity of the source and recipient of the communication;

28 Clause 26(5).
(ii) Service use: this tells you how a communication occurred (i.e. was it via email, a text or a phone call etc), the date and time it occurred and how long it lasted;

(iii) Subscriber information: this tells you any information held by the person who has signed up to the communications service, for example the name and address and any direct debit details of the user.

Access

26. RIPA provides, on the face of the Act, for all forms of communications data to be available to the intelligence services, the police, the Serious Organised Crime Agency (SOCA), HMRC and other specified public authorities provided for by order; these include the Financial Services Authority, the Gambling Commission and the National Health Service Trust. The power to acquire service use data and subscriber information is available to over 430 local authorities and a significant number of other public authorities, including the Food Standards Agency, the Charity Commission and the Environment Agency. The permitted purposes for which communications data may be accessed are broad and ill-defined, including in the interests of the economic well-being of the UK and to assess or collect any tax, duty or other type of government charge. The Act provides for a regime of internal authorisation for access to communications data for a large number of public bodies. Section 37 of the Protection of Freedoms Act 2012 amended RIPA to require prior judicial authorisation for access to communications data by local authorities however this section is not yet and even once in force, will only affect a small fraction of communications data requests.

---

29 For the full list see the Regulation of Investigatory Powers (Communications Data) Order 2010, Schedule 2, Part 1.
30 For the full list see the Regulation of Investigatory Powers (Communications Data) Order 2010, Schedule 2, Part 2.
31 See section 22 of RIPA. Communications data can also be accessed in an emergency to prevent death or to prevent or mitigate injury or any damage to a person’s mental or physical health. For the types of surveillance local authorities have access to, the Secretary of State can make orders extending the purpose for which authorisations can be made. To date orders have been made to allow communications data to be accessed to investigate alleged miscarriages of justice and to assist in identifying deceased persons or persons unable to identify themselves because of a physical or mental condition. See Regulation of Investigatory Powers (Communications Data) Order 2010, SI 480/2010.
32 Section 37 of the Protection of Freedoms Act has not yet been brought into force.
Availability

27. While communications service providers (BT, Virgin etc) typically retain some information about their customers’ past use of communications for their own business purposes (e.g. itemised phone bills) they were not – until relatively recently - obliged to retain any such data about their customers.

28. A small shift in this area took place in 2001 when the Anti-Terrorism Crime and Security Act was rushed through Parliament following the tragic events of 9/11. Amid a host of draconian anti-terror powers stood Part 11, providing for the creation of voluntary agreements between service providers and the Government for the extended retention of communications data The internet initially objected to these voluntary agreements, with the Secretary General of the Internet Providers Association informing then Home Secretary, Rt Hon David Blunkett, that the industry was not convinced that extending the length of time companies hold on to customer logs was necessary for the fight against terrorism and organised crime.33 In July that year the Information Commissioner publically warned the Home Office that plans for a voluntary code of practice for the retention of communications data could violate human rights protections because logs supposedly retained for the purposes of serious criminal investigations could be accessed for such purposes as the levying of taxes.34 The Foundation for Information Policy Research also came out in opposition, warning of the dangers of a policy rejected by ‘civil society, Europe’s data protection commissioners and now internet service providers’.35

29. Notwithstanding widespread concerns about the impact of a proposed voluntary code, in 2003 the Home Office, secured a series of agreements with service providers. To date we do not know the details of these agreements nor do we have confirmation of the parties involved. These initial agreements related to information already kept for commercial purposes, establishing a minimum period for retention.

30. In 2002 the Home Office attempted another policy to extend access to communications data to a wide range of public authorities – authorities with no law enforcement remit whatsoever, including parish councils. In the face of huge opposition, these plans were scaled back, however the RIPA regime still grants access to a huge range of public authorities on the basis of a process of internal authorisation.

31. Still dissatisfied with capabilities in this area, in 2005 the Home Office used the UK presidency of the EU to push through compulsory arrangements for communications data retention which resulted in the EU Data Retention Directive 2006.\(^{36}\) The Directive provides for the mandatory retention of communications data (already retained for billing or commercial purposes) for between 6 and 24 months. Sweden postponed the implementation of the Directive facing huge fines, whilst across EU member states cases were brought challenging the domestic legislation transposing the Directive.\(^{37}\)

32. Back in the UK and before the transposing legislation had even come into force, the Home Office ‘Interception Modernisation Programme’ (IMP) was already in train. The Government declared an intention to bring forward legislation, a ‘Communications Data Bill’ in 2008-2009.\(^{38}\) Initial proposals were premised on the construction of a centralised database, but these plans were hastily dropped in favour of a series of industry controlled mini-databases. Opposition to the explosion in state surveillance facilitated by the last Government was pronounced, with Liberal Democrat Leader Nick Clegg observing of the last Labour Government, in February 2008, that ‘it is this Government that has turned the British public into the most spied upon on the planet.’\(^{39}\)

33. In April 2009 the UK fully transposed the Directive by way of the Data Retention (EC Directive) Regulations 2009 (‘the regulations’), which provide for requirements to be placed on service providers to retain communications data kept ordinarily for commercial purposes for a minimum of 12 months. We still do not know which UK based communications companies are required to retain our data; requests for disclosure are met with the familiar refrain that information cannot be revealed for


\(^{37}\) Explored further at paragraphs 64-68 below.


\(^{39}\) Hansard, 6 Feb 2008 : Column 951.
reasons of national security.\textsuperscript{40} Two months later in June 2009, the Home Office launched its consultation ‘Protecting the Public in a Changing Communications Environment’.\textsuperscript{41} Having rejected plans for a centralised database, the resulting proposals strongly resemble those which now form the Draft Communications Data Bill. Then Home Office Minister Lord West stated that ‘the objective of the IMP is to maintain the UK’s lawful intercept and communications data capabilities in a changing communications environment.’\textsuperscript{42} In its response to the consultation, the UK’s largest communications service provider, BT, pointed out that:

‘[t]he proposals would outsource data collection, processing and retention to CSPs rather than building a central Government database and could result in significant brand, reputation and customer relationship issues for CSPs… retaining data on the scale proposed would raise significant issues of proportionality, especially in view of the fact that only a fraction of the data might be used. Moreover, finding the pieces of information that might prove to be useful to the relevant authorities amongst the mountain of data that will be available to them will be no easy task – the proverbial “needle in a haystack”.’\textsuperscript{43}

In June 2009, the same month that the consultation was launched the Leader of the Conservative Party, David Cameron, argued that ‘today we are in danger of living in a control state. Every month over 1,000 surveillance operations are carried out. The tentacles of the state can even rifle through your bins for juicy information.’\textsuperscript{44}

\textsuperscript{40} The Data Retention (EC Directive) Regulations require the Secretary of State to give notice to those telecommunication providers he or she wishes to retain data. In 2009 a Freedom of Information Request was submitted to the Home Office requesting information regarding the identity of those service providers which had received notices under regulation 10 of the Regulations. This request was refused by the Home Office and the related correspondence is available at: http://www.whatdotheyknow.com/request/notices_under_regulation_10_of_s


\textsuperscript{42} Hansard, 8 July 2008 : Column WA76.


\textsuperscript{44} Speech by Rt Hon David Cameron, Giving Power Back to the People, 25\textsuperscript{th} June 2009, available at: http://www.conservatives.com/News/Speeches/2009/06/David_Cameron_Giving_power_back_to_the_people.aspx
34. Liberty was amongst the many groups and individuals, including service providers and other industry bodies who expressed concerns at these proposals and in light of widespread opposition, Labour shelved the project in November 2009. Notwithstanding the Coalition’s commitment, in July 2010 the first signs of a u-turn emerged as the Home Office, in a ‘Draft Structural Reform Plan’, stated that it would ‘publish proposals for the storage of internet and email records, including introducing legislation if necessary’. By October 2010, the Government’s plans had apparently solidified into an attempt to revive the discredited IMP, with the Strategic Defence and Security Review outlining – amongst a wide range of other proposals - plans to ‘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’.

**Key changes proposed to the current regime**

35. The Draft Bill would change current arrangements for the retention of communications data in three significant ways:

(i) First, under the Draft Bill, unprecedented requirements may be placed on UK based operators to collect and process communications data generated by web-based services such as Gmail and Facebook, provided by overseas operators, which cross their domestic networks. It is widely suggested that the only way to obtain such information, in the absence of voluntary agreements with third party providers, is through Deep Packet Inspection (DPI) technology. According to one leading expert, whilst DPI can operate as software, when traffic levels are high specialised hardware must be installed which captures a data stream as it crosses an operator’s network.

(ii) Second, the definition of those bodies required to retain data is significantly wider covering all ‘telecommunications operators’ (‘operators’) as opposed to the ‘public

---

47 Clause 1(3)(c)(ii).
48 Submission of Professor Peter Sommer to the Joint Committee on the Draft Communications Bill, para 41.
communications providers' referred to in the retention regulations. An operator is ‘a person who controls or provides a telecommunications system, or provides a telecommunications service’. This includes all telecommunications companies BT, Orange, TalkTalk, Vodafone and others, but would also extend to manufacturers of communications equipment who could be called upon to adapt their products with the aim of facilitating access to communications data, and to private networks for example blackberry messenger or internal ‘intranet’ operators in private companies or other organisations. Requirements could also be placed on anyone who owns a mobile phone or other telecommunications equipment including a private individual.

(iii) Third, the Bill makes provision for central filtering arrangements to be operated by the Home Office. The central filter will bring together atomised pieces of data to create a revealing whole which can be disclosed to public bodies in response to specific requests. Whilst not a comprehensive central database in itself, this is a co-ordinated Government operated facility through which many requests for data will be processed. The privately operated databases will be joined up to create an integrated system. This regime raises many of the same concerns as a large and centralised store and no details are given about security arrangements, or the clearly envisaged human involvement in what the Government describes as an ‘automated system’. Further the filtering arrangements provided for in the Bill throw into sharp focus the depth and breadth of the information which can be gleaned through a comprehensive system of data retention combined with substantial and sophisticated processing arrangements. The Government has laboured the distinction between content and communications data; its case is that the privacy implications of the later are small by comparison. Yet the central filter will provide for vast swaths of data, retained by disparate companies, to be scanned for relevant information, connected up and shaped into a coherent and acutely revealing whole – data can be matched up to reveal a huge amount about an individual’s life in order to work out whether a request made by a designated senior officer is necessary and proportionate. The Bill anticipates the kind of advanced processing, shaping and linking of data provided for in the filtering arrangements to take place as a precursor to establishing the necessity of access. This carries huge potential for in-depth processing of the data of innocent individuals – individuals who will likely never know that their data has been handled in this way and are consequently deprived of any opportunity to mount a challenge.

\[49\] Clause 28.
36. The Draft Bill contains substantially the same provisions for access as provided for under RIPA as amended by section 37 of the *Protection of Freedoms Act* 2012. Aside from the four enforcement agencies provided for on the face of the Draft Bill which mirror provision in RIPA, details about the public authorities, including local authorities which will be permitted to access data will be provided in secondary legislation expected to reflect the provisions of the *Regulation of Investigatory Powers (Communications Data) Order* 2010. As at present, local authorities will not have access to traffic data and access to traffic data by other public authorities (outside of those listed in the Bill) will be governed by Secretary of State order. Scrutiny arrangements provided for under the Bill substantially mirror those provided for in RIPA.\(^{50}\)

**The civil liberties implications of blanket data collection**

37. The civil liberties concerns around this Draft Bill relate to all three of its component parts: data collection, access and scrutiny – additional concerns around the processing of data in a central filter which span collection and access also carry significant privacy implications.

38. Much attention has been given to the proposed access arrangements provided for in the Draft Bill which largely mirror those already in existence. Liberty agrees that pressing concerns exist in this area and these concerns intensify as the pool of data retained increases. However we believe that the more fundamental danger of this Draft Bill is the provision it makes for a shift from limited data retention to blanket data collection.

39. The Government's attempted justification for requiring the blanket collection and retention of communications data is based on four highly questionable assumptions which we will examine in turn, first that communications data is not particularly revealing, second that communications data can always be practically and conceptually distinguished from content, third that blanket retention of communications data will lead seamlessly to gains in law enforcement and finally that requiring blanket collection of this information will do no more than “maintain capability”.

\(^{50}\) See, Chapter 2 of Part 1 of RIPA, in particular section 57.
40. The Government argues that communications data is less revealing than data generated by, for example, interception or bugging, and that this justifies a considerable divergence in approach to that taken with other targeted surveillance powers. This assumption is highly questionable. Communications data can build up an incredibly intimate picture of our lives. With the proliferation of mobile forms of communication, in addition to tracing the timing, duration, recipient and source of a communication, specific details about an individual’s location can also be collected. When combined with substantial subscriber information, the revealing nature of communications data is hard to dispute. Compile and co-ordinate this information for every call, text, email, tweet, blog and Facebook posting and you have a map of our daily routines, our relationships, our habits and preferences, the streets we walk, where we work and socialise, the extent and nature of our communications with others. Furthermore, consider the range of situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a Times reporter immediately before a major whistleblower scandal fills the front pages, the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody. The record of a website visited, which falls firmly within the definition of communications data, can also be incredibly revealing. Consider, for example, the case of a teenager viewing an abortion website, a celebrity accessing the website of an HIV service provider. We must not underestimate the intrusion that the retention of communications data, without more, represents.

41. In April this year, in response to the disclosure of further details of the Government’s plans to extend the collection of communications, Sir Tim Berners-Lee, inventor of the world wide web, came out in opposition to the proposals. In an interview with the Guardian he stressed that the planned extension of the state’s surveillance powers would make a huge amount of highly intimate information vulnerable to theft or release by corrupt officials, adding that:

"The amount of control you have over somebody if you can monitor internet activity is amazing. You get to know every detail, you get to know, in a way, more intimate details about their life than any person that they talk to because often people will confide in the internet as they find their way through medical websites … or as an adolescent finds their way through a website about
homosexuality, wondering what they are and whether they should talk to people about it.  

42. The Internet Service Providers Association has also joined the building opposition to these proposals pointing to its concerns ‘about the new powers to require network operators to capture and retain third party communications data… [including] the scope, proportionality, privacy and data protection implications and the technical feasibility.’  

According to a report in the Independent, after being informally briefed by Government earlier this year, the Association expressed concern that ‘network operators are going to be asked to put probes in the network and they are upset about the idea… it’s expensive, it’s intrusive to your customers, it’s difficult to see it’s going to work and it’s going to be a nightmare to run legally.’  

Blurring of record and content of communications  

43. At one time a firm distinction between communications data and content would have been more credible, for example when much communication was by letter: everything inside the envelope is content, everything on the outside communications data. To say that things are no longer so simple is a significant understatement. The proliferation of innovative new forms of online communication and the resultant fragmentation and diversification has created a complex and multifaceted communications landscape. In support of its argument that technology is making the RIPA definitions of communications and interception more and more difficult to sustain, the LSE, in a study examining remarkably similar proposals put forward by the last Government, observed:

Historically there have been two entirely separate regimes for authorising access to [communications data] and for intercepting content. We strongly

---

doubt that this framework can be maintained in the new ICT environment of web-based email, social networking, online gaming and cloud computing.\textsuperscript{54}

We do not pretend to be technical experts. We do however understand that there are increasing practical difficulties within new technologies in distinguishing communications data from content and perhaps more disturbingly in recording communications data without capturing content.

44. Communications services are now provided by a host of companies based all over the world. Web-based services such as webmail and social networking sites dominate the communications landscape. The domestic companies who provide our internet access, for example BT, TalkTalk or Virgin, are no longer the companies which provide the most widely used email services such Gmail and Hotmail or social network sites like Facebook or Twitter. Details of these communications are not routinely retained by those that bill us because we are charged periodically for access, rather than for each use of a service. Despite Home Office claims that this Draft Bill is about working collaboratively with operators, including those based overseas, we have no clear picture of the extent to which, for example, webmail providers like Google collect or retain communications data generated by service users, never mind their willingness to hand this information over. The Home Office acknowledge that where voluntary agreements are not forthcoming, other arrangements will be put in place to ensure data collection and retention. Our understanding is that as traditional communications service providers like BT become increasingly a mere vehicle for accessing other web-based services the centrality of Deep Packet Inspection (DPI) technology to the system as a whole becomes inescapable.

45. DPI is the generic name for the equipment that would be required for the collection and analysis of third-party data. The LSE’s study into the last Government’s Interception Modernisation Programme maintains that every use of DPI is in fact an interception, even if its purpose is to gain access to communications data.\textsuperscript{55} DPI ‘black boxes’ capture the entire data stream, computer programmes or ‘scripts’ are then written in order to extract the description of data required.\textsuperscript{56} By requiring UK based operators to install DPI black boxes on their lines to capture

\textsuperscript{54} LSE Briefing on the Interception Modernisation Programme, page 3.
\textsuperscript{55} Ibid, pg 22.
\textsuperscript{56} Ibid, pg 37.
every data stream which crosses their networks, this Draft Bill provides for the creation of the physical infrastructure for the interception and retention of all of our communications. If we accept that effective programmes or ‘scripts’ can be written which discard the content and collect the communications data, we cannot avoid the fact that, with a reformulation of these programmes, the nature of the data retained could be dramatically altered. What is more, the LSE also describes how black boxes which contain DPI software can be programmed and re-programmed remotely. Ultimately there is nothing to stop another administration from bringing forward legislation which makes fuller use of the new capability which will be created by the proliferation of DPI black boxes.

46. Liberty believes that a number of obvious unanswered questions arise around the use of this technology, for example who will exercise effective control over DPI boxes? Who will write the programs or ‘scripts’ which dictate those aspects of the data that are to be retained and those parts which will be discarded? What are the technological and cost implications of ensuring that software installed and programs written keep pace with the technological advancement including new forms of internet based communication? Will organised criminals be able to evade detection by using encryption or anonymisation techniques, hijacking the poorly secured internet connections of others or changing the IP address of a computer moment by moment? Further some technology experts have warned that modern communications are so complicated that it may be impossible to separate out the basic contact data from the content in terms of the data retained.

Law enforcement gains?

47. Our ability to comment on potential law enforcement gains of blanket collection is restricted by the unanswered questions which remain around the role of communications data in law enforcement and other areas. We still do not have a full picture, across all those public bodies able to access communications data, of the types of investigation for which data is accessed, the extent of access and the number of individuals affected. We are told that, over the past decade, communications data played a role in 95% of all serious criminal investigations, but

we have no idea about the extent of this role. Was communications data central to the operation or a peripheral detail? How many of these investigations led to successful prosecutions? Could the prosecution have been secured without access to this data? Further in how many low level, non-serious and even non-criminal investigations is communications data used? A recent freedom of information request involving Humberside police revealed that a residual category for communications data access requests is ‘other non-crime’. 59

48. The Government’s argument assumes that further collection of communications data will lead seamlessly to better law enforcement, however the collection and storage of yet more personal information also brings risks. In recent years the government has lost 25 million child benefit records as well as the personal information of those serving in the armed forces, witnesses in criminal cases and prisoners. Further communications data collection and retention necessarily means that the data will pass through more hands and potentially be more susceptible to bureaucratic error and even fraud. Communications data can be just as interesting and revealing as intercepted content and in the aftermath of the phone-hacking scandal we should be particularly wary of create new targets for abuse and misuse.

49. In other countries reports of unlawful interception should serve to caution us against the creation of the infrastructure for the interception of all our communications. In Greece in recent years the unlawful use of interception capability was widely reported. The scandal reportedly involved wiretapping of Eriksson software used by Vodafone which had the capability to intercept communications data albeit that was not the primary purpose for which it was used. We understand that the hackers operated in such a way that it wasn’t clear the intercept capabilities in the software were being used and their activities reportedly went undetected from August 2004 until January 2005; they were finally shut down in March 2005. 60

59 See evidence to the Draft Communications Data Bill Committee on Wednesday 11th July: “Humberside police confirmed that they have used this nearly 200 times in three years for traffic offences, and terrorism is not listed as one of the crimes, they even beautifully list the category ‘other non-crime’.” Nick Pickles, Big Brother Watch.
60 The scandal was reported in the Wall Street Journal on 21 June 2006: “In early March 2005, George Koronias, Vodafone Group PLC’s top executive here, contacted the Greek prime minister’s office about an urgent security matter. Vodafone’s network in Greece had been infiltrated by phone-tapping software targeting an elite group of cellphones: those assigned to many of the country’s leaders, including senior police and defense officials, cabinet members and the prime minister himself.” For more see: http://online.wsj.com/article_email/SB115085571895085969-LMyQjAxMDE2NTIwMTgyNTE1Wj.html.
50. Similarly in Italy a multifaceted wiretapping scandal reportedly involving Telecom Italia ranged from 1996 until it was finally uncovered in 2006. A fresh and apparently unrelated wiretapping scandal in which Telecom Italia was also implicated emerged in 2007. Both scandals were reportedly huge, complex and have still not been fully uncovered; it has been variously alleged that they involved intelligence services and were bound up in state surveillance and security, terrorism and rendition, as well as corporate infighting. The original, long running scandal involved the exploitation of a flaw in Telecom Italia’s security systems, which allowed a person to set up wiretaps without leaving any trace. The phones of politicians and other high-profile politicians were reportedly tapped using existing infrastructure.61

51. According to the LSE multiple vulnerabilities in the infrastructure for the retention of communications data have reportedly been uncovered in the US that ‘would allow adversaries to take them over and perform unlawful interception.’62 Securing the configuration of devices to protect against unwarranted intercept will be a matter of the utmost importance, but to date we have little information about the arrangements to be put in place to protect against security breaches. The scope of these proposals throws the potential implications of a breach into sharp focus.

52. The Interception of Communications Commissioner’s latest report provides further cause for concern. During 2011 public authorities as a whole submitted 494,078 requests for communications data, 52% of these requests were for subscriber data, 25% for traffic data and 6% for service use data – 17% of requests were for a combination of different sorts of data.63 During 2011, 895 communications data errors were reported, with approximately 80% of those attributable to public authorities and 20% to Communications Services Providers.64 This included 99 identified by the Commissioner’s Office from the small sample of cases reviewed.65 In a report a good deal fuller and more detailed than in previous years, the

62 See Ibid, pg 26: ‘Studies of interception equipment conforming to the US communications surveillance standards (under ‘CALEA’) were in the past found to contain multiple vulnerabilities that would allow adversaries to take them over and perform unlawful interception.’
63 Interception of Communications Commissioners Annual Report to the Prime Minister 2011, Chapter 7, pg 28-29.
64 Ibid, pg 30.
Commissioner also referenced two cases in which individuals were arrested, wrongly detained and accused of crimes on the basis of data errors, further communications data had been illegitimately used by a local authority to determine whether a family lived in the right school catchment area. 0.4% of annual requests for communications data are made by local authorities.

53. Despite reiterated warnings about the diminishing capabilities of the State as regards communications data little mention is made of current loopholes in capability or the extent to which they would be left unchanged by the proposals. Our understanding is that there has and will always be methods of communication that do not come within the State’s reach and these are just as likely to be methods of relatively little sophistication as well as those of greater sophistication. One example is the use of unregistered pay-as-you-go mobile phones. In reviewing the future communications landscape it is reasonable to suggest that truly sophisticated criminal networks will continue to make use of readily available anonymised methods of communication.

Extending rather than maintaining capability

54. In evidence before the Committee, in addition to in the explanatory notes and impact assessments accompanying the Draft Bill, the Home Office reiterates its claim that projected technological changes will decrease the State’s capability as regards the use of communications data. While it is difficult to argue with the substance of the technological changes projected, the description given is notable for what is missing. Technological innovation has, and will continue to, reap huge gains for law enforcement in the UK but the Government makes no attempt to present the current proposals in historical context. By this we do not suggest that a protracted discussion of telephony or other technological innovations is required – rather some reference to how the ability to access records of communications between individuals is, in itself, a recent boon for law enforcement would give a much fuller picture of where we currently stand. Not too long ago, before the wide availability of mobile phones and email, most communications between individuals, if not carried out through traditional telephony or letter writing, would have been conducted face to face. This would have presented different - potentially more challenging - obstacles to law enforcement.

67 Ibid, pg 43.
68 Ibid, pg 39.
Just because in recent times the State has benefitted from access to communications data that was already recorded and retained by communications providers does not mean that total access to all communications data should be required, for all time, regardless of cost and implications. Further, it does not follow that just because communications data can be recorded and historic records made available that they should. For good reason other - supposedly more intrusive - surveillance techniques available under RIPA such as bugging (whether in private or in public), the use of human covert surveillance or the interception of communications need prior authorisation on the basis of individual suspicion. Once authorised they can only be carried out in the future. The Government is not presently arguing that we should all be routinely or randomly subject to bugging, covert tracking or interception ‘just in case’ but, if the present proposal is allowed to pass, proposals for other types of blanket or random surveillance irrespective of suspicion “just in case” are a logical next step.

*Impact on freedom of expression and assembly*

55. In addition to the very obvious privacy implications, it is important to remember that proposals of this nature engage other fundamental human rights, most notably the right to freedom of expression as protected by Article 10 of the ECHR and freedom of assembly as protected by Article 11. We need only look at the role of social media in organising the protests that have precipitated the spread of democracy across the Middle East, to realise that freedoms central to the promotion and preservation of democracy, freedom of expression and freedom of assembly in particular, are engaged by measures providing for the blanket collection of information about the web habits of the population at large. Freedom House’s 2011 Freedom on the Net Report, observes that:

*In Egypt and Tunisia, for example, democracy advocates have relied heavily on Facebook to mobilize supporters and organize mass rallies. Similarly, Bahraini activists have used Twitter and YouTube to inform the outside world about the government’s violent response to their protests. Even in Cuba, one of the most closed societies in the world, several bloggers have been able to report on daily life and human rights violations.*

---

56. In Saudi Arabia, a country where freedom of expression is strictly circumscribed, online activists have been able to expose corruption and hypocrisy amongst the ruling royal family.\textsuperscript{70} Similarly internet users in Thailand have played a significant role in challenging the ruling elites since the Thai military coup of 2006.\textsuperscript{71} In Russia and Venezuela with restrictions on broadcast media outlets growing, the internet has been seized upon by those seeking to demonstrate their dissatisfaction with the regime and mobilize opposition.\textsuperscript{72} The potential created by the internet for empowering ordinary citizens and giving a voice to the voiceless is arguably one of the most inspiring developments of recent history.

57. In our developed democracy too, the internet has had a huge role to play in the flourishing of democratic participation. Democracy requires free and fair elections, but it does not stop there. The internet has given ordinary people a forum to contribute to debates of national significance, organise peaceful protest on a large scale and put real and immediate pressure on our political representatives. Grassroots activism aside, the internet has also given the whole population the ability to communicate in innovative new ways with loved ones no matter where in the world they are, it has allowed people to nurture friendships, develop contacts, share ideas and reach out to everyone or anyone about the issues that matter to them. Never before has the right to speak your mind been so real as in the internet age.

58. Repressive regimes throughout the world have felt justifiably threatened by the empowering impact of the web. Techniques employed to stifle online freedom include blocking huge areas of content and filtering access to every area of the web within a jurisdiction.\textsuperscript{73} Widespread monitoring is also a technique used by some regimes to limit the capacity of the internet to effect social change. Freedom House reports that:

\textit{The Iranian authorities have taken a range of measures to monitor online communications, and a number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news.}\textsuperscript{74}

\textsuperscript{70} Ibid, pg 289-291.
\textsuperscript{71} Ibid, pg 9.
\textsuperscript{72} Ibid, pg 9-10.
\textsuperscript{73} Ibid, with China, Cuba and Iran amongst the worst culprits see pg 23, 24 and 26 in particular.
\textsuperscript{74} Ibid, pg 26.
59. One way many oppressive regimes have opted to control the internet is by requiring communications services providers to further a repressive agenda. After social networking sites facilitated pivotal protests in Egypt, the authorities directed internet service providers to remove pathways for computer users to connect to requested websites, whilst in Iran tactics include ordering the removal of posts deemed offensive from the sites of blogging service providers. Zimbabwe’s 2007 Interception of Communications Act allows the authorities to monitor telephone and internet traffic, and requires service providers to intercept communications on the state’s behalf. It is very difficult to accurately assess the scope of internet controls employed by secretive authoritarian regimes, but what is clear is that monitoring web-activities in various ways is a vehicle for curtailing the flow of ideas which may ultimately lead to social change.

60. If the scheme envisaged in the Draft Bill is brought into force, we will distinguish ourselves amongst European countries as the leaders in online surveillance and earn a place on a spectrum including some of the most oppressive regimes in the world. Liberty believes that the knowledge that details of web habits are collected on mass with the possibility of future access ever present, will create a real shift in online behaviour. There are many different ways to curtail freedom of expression online, mass collection of information whether carried out by the state or simply orchestrated by Government and operated by the private sector is one of those.

61. As well as an attack of the place of free expression in our wider social fabric, the spectre of online surveillance will have very real and specific impacts, for example on journalists, whistleblowers and trade unionists. The protection offered by Article 10 covers journalistic sources – one of the ethical cornerstones of reporting. The centrality of journalistic sources to a free media was fully endorsed in a case involving the Financial Times in 2001. Attempts to force the newspaper to disclose its sources were ultimately defeated in recognition of the real potential chilling effect on press freedom. In another stark example of the role of data collection in stifling freedom of expression and freedom of assembly, Liberty recently took up the cause of thousands of workers whose details were stored on a secret database discovered

---

75 Ibid, pg 7.
76 Ibid, pg 26.
77 Financial Times Ltd and Others v United Kingdom (Application no. 821/03).
three years ago. Full details of the information collected are still emerging, but amongst the data stored was information indicating a history of trade unionism.\textsuperscript{78} An official from the Office of the Information Commissioner reportedly told a Tribunal that some of the information could only have been supplied by police or the security services.\textsuperscript{79} A significant number of major firms allegedly used the information in making recruitment decisions. Data collection on the scale proposed can only add to the risk that scandals of this type will be repeated.

\textbf{Unlawfulness of blanket communications data collection/retention}

62. Proposals to collect and retain records of all electronic and postal communications necessarily engage the right to respect for private and family life protected by Article 8 of the European Convention on Human Rights as protected by our \textit{Human Rights Act} 1998 (the HRA). As with most HRA rights, the right to private life can be limited where the limitation can be shown to be necessary and proportionate to satisfy the legitimate aim of preventing and detecting crime as well as other social interests. Whilst communications data is undoubtedly useful in crime detection it does not follow that collecting and retaining all communications data between all individuals is proportionate. Still less that processing communications data \textit{just in case} would satisfy requirements of necessity and proportionality which are central to the protection of personal privacy in this country. The law enforcement implications are at best unclear, the security risks great and the intrusiveness of communications data incontrovertible.

63. As a result of the Data Retention Directive, the current regime across Europe allows for the retention of certain communications data by communications service providers for a fixed period. The draft Communications Data Bill would extend the law beyond the Directive. As such, cases on the Directive are highly instructive: If the Directive is disproportionate under human rights laws, then the Communications Data Bill must be too.


\textsuperscript{79} The Independent: \textit{Thousands of workers ‘blacklisted’ over political views}, Tuesday 7\textsuperscript{th} August. Available at: \url{http://www.independent.co.uk/news/uk/home-news/thousands-of-workers-blacklisted-over-political-views-8010208.html}. 
64. Constitutional courts across the Continent have declared that the present EU regime for retention of records violates basic rights and freedoms. In October 2008, the Romanian Constitution Court became the first to declare legislation transposing the EU Directive in breach of its Constitution. The Court found that the mandatory retention of communications data scheme engaged a number of fundamental rights, namely the right to freedom of movement, the right to intimate, family and private life, privacy of correspondence and the right to freedom of expression. In finding its transposing legislation disproportionate, the Court relied on, amongst other issues, the reversal of the ordinary presumption of innocence and the lack of a reasoned basis for the retention period required, finding also that retention on the scale required was 'likely to prejudice, to inhibit the free usage of the right to communication or expression'.

Two months later the Bulgarian Supreme Administrative Court followed suit, finding its own enabling legislation incompatible with the country's constitutional protection of personal privacy.

65. In March 2010, Germany's Constitutional Court declared the provisions of its law transposing the Directive unconstitutional. In finding the communications data retention regime incompatible with constitutional protection for personal privacy, the Court commented that 'the protection of communication does not include only the content but also the secrecy of the circumstances of the communication, including if, when and how many times did some person... contact another.' The Court went on to find that 'the evaluation of this data makes it possible to make conclusions about hidden depths of a person’s private life and gives under certain circumstances a picture of detailed personality and movement profiles; therefore it can not be in

---


general concluded that the use of this data presents a less extensive intrusion than the control of the content of communications. 63

66. The Cypriot Constitutional Court in February 2011 ruled orders issued under its transposing law unconstitutional 84 and in March the same year the Czech Constitutional Court annulled transposing legislation, expressing doubt as to whether such widespread retention of data was necessary or even effective. 85 A case is pending before the Hungarian Constitutional court which involves a challenge to transposing legislation surrounding the depth of data processing. 86

67. 2012 has seen more questions raised around the legitimacy of the EU regime, with a leaked European Commission paper setting out doubts as to the legality and utility of the Directive. 87 In this document, the Commission acknowledges the lack of support for the Directive’s crime-tackling aspirations and points to the vagaries of the scheme. The legality of the Directive is now set to be challenged directly under Article 8 of the European Convention on Human Rights as well as parallel provision in the EU Charter, in the case of Digital Rights Ireland referred to the European Court of Justice (ECJ) by the High Court in Ireland. 88 In this preliminary reference, the High Court specifically ask whether the Directive is compatible with Article 7 of the EU Charter/Article 8 ECHR (rights to privacy); Article 8 Charter (protection of personal data); and Art 11 Charter/Article 10 ECHR (freedom of expression). The Digital Rights Ireland case will be hugely significant for the future of the present data retention framework as well as for the Draft Bill under consideration. It is startling therefore that the UK Government is not willing to wait for the decision in this important case before pressing ahead with even more intrusive rules. Assuming the ECJ clearly answers all the questions posed by the High Court, the implications of the case will be highly important. If the Court takes the same line adopted by so many national constitutional courts, then the Directive may be annulled on grounds of proportionality and breach of human rights. Such a decision could pave the way for a

---

83 Ibid.
successful legal challenge to the lawfulness of the present regime in the UK courts and would seriously undermine government arguments about the need and legitimacy of going further under the draft Communications Data Bill.

68. Liberty believes that the present framework for communications data retention is in breach of Article 8 and that the proposals contained in this Draft Bill – which necessarily go much further - would put the UK further in breach. An analogy can be made with the retention of DNA. It is uncontroversial to say that DNA profiles can be incredibly useful in detecting and preventing crime. That is not to say that a universal DNA database would be desirable. Indeed the creation of a universal DNA database would be a disproportionate means of achieving the legitimate aim of crime detection and prevention. This was confirmed in the judgment in \textit{S and Marper v UK} in December 2008 and reflected in the revising provisions of the \textit{Protection of Freedoms Act 2012}.\footnote{See Part 1 of the \textit{Protection of Freedoms Act 2012}.} There now appears to be a general acceptance of the fact that the last government’s policy of indefinite, blanket retention of the DNA of all those arrested was unlawful and unacceptably detrimental to personal privacy.

\section*{Review of RIPA}

69. While the original intention of RIPA was to bring the UK better in line with universally recognised human rights standards, the legislation which resulted and developments since mean that its review and revision is long overdue. Liberty has long called for an overhaul of the RIPA framework so that safeguards can be incorporated that better protect those in the UK from unnecessary and heavy handed surveillance.

\subsection*{Access arrangements}

70. Liberty supports the amendment to RIPA contained in the \textit{Protection of Freedom Act 2012} which requires prior judicial authorisation in some areas of communications data access. This reform is replicated in the Draft Bill. Whilst the inclusion of warranty requirements for local authority access is welcome, it does not address concerns about the additional capacity authorised by this Bill and the swathes of additional, revealing data which will be retained. Further the impact of limited provision for judicial authorisation should not be overstated, given that local
authorities account for only 0.4% of requests for access to communications data. The latest Report of the Interception of Communications Commissioner reveals that, during 2011 only 141 of 400 local authorities able to access communication notified the Commissioner that they had made use of their powers. 79% of these local authorities made less than 20 requests, 58% less than 10. Given the relatively small numbers involved, and the limited nature of a local authority law enforcement capacity, Liberty questions the need for any local authority access to communications data.

71. The purposes for which data can be accessed by local authorities or other relevant public authorities remain unnecessarily broad and ill-defined. No definition is given as to what is, for example, ‘in the interests of national security’ or the ‘economic well-being of the UK’. We do know, however, that the last government took an alarmingly expansive view of what may be justified in the name of the ‘economic well-being of the UK’ arguing on one occasion that restricting drug-users access to welfare benefits is justified to further that aim. In evidence to the Committee, Charles Farr, the Director of the Office for Security and Counter-Terrorism at the Home Office, refused to rule out access to communications data for the purpose of identifying those caught speaking on the telephone whilst driving. Human rights standards require that in the exercise of surveillance there must be adequate safeguards to protect the citizen against excessive intrusion or other abuses of rights. The use of broad and vague notions such as ‘national security’ and ‘economic well-being’ give rise to a real risk that the disproportionate use of surveillance will be authorised, going beyond what is necessary to protect the public from harm. This could interfere unacceptably with political and other lawful activity that ought to go unimpeded in a democratic society. We believe that these grounds should be better defined, particularly as the prevention or detection of crime, or serious crime, is already included which should capture the majority, if not all, of the grounds on which surveillance needs to be authorised. The ability of the Secretary of State to expand the list by order also contrasts with the prescriptive nature of Article 8. This raises serious concerns over the compatibility of RIPA powers with the right to respect for personal privacy.

90 Ibid, pg 39.
91 Ibid, pg 38.
92 Ibid pg 39.
94 See Evidence to the Committee on Tuesday 10th July.
72. Liberty has ongoing concerns about the process of self-authorisation which currently applies across the board and remains in place for all those public authorities listed on the face of the Bill and, subject to provision to the contrary in secondary legislation, all other public authorities (save for local authorities) to whom access is granted. Under the Draft Bill other public authorities included in the access regime will continue to operate a system of internal authorisation. Senior police officers and Home Office officials claim that the designated senior officer authorising access to communications data will not be somebody involved in the particular operation or investigation for which the information is sought. It should be noted, however, that the Draft Bill makes explicit provision for a designated officer to authorise his own access to communications data and places no restrictions on his ability to authorise access by reference to the extent of his involvement in the investigation concerned.\textsuperscript{95} The Code of Practice which currently governs access to communications data specifically deals with this issue and whilst maintaining that ‘designated persons should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved’, this assertion is substantially undermined by the caveat ‘although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons’.\textsuperscript{96}

73. Liberty maintains that even if a designated officer is not directly involved in an investigation it is entirely unacceptable for public authorities to be able to self-authorise access to revealing personal data, particularly when the access regime is so broadly framed. Considerations of necessity and proportionality should be assessed by a member of the judiciary who will be both independent and adept at conducting the Article 8 balancing exercise. We do not seek to impugn the integrity of senior employees of our law enforcement agencies, but rather point out the reality that their primary concern will relate to the operational capacity of their agency. This is a matter of organisation culture and is perfectly understandable, but it is also a reality which mitigates in favour of independent third party authorisation.

74. In the cases of those organisations which do not routinely access communications data, our concerns are greater still. A public official within a public

\textsuperscript{95} Clause 9(2).
\textsuperscript{96} Home Office Code of Practice for the Acquisition and Disclosure of Communications Data, paragraph 3.11.
authority that may not exercise such powers on a regular basis is hardly well placed
to determine when conduct will or will not unnecessarily or disproportionately
interfere with a person's privacy. We are further concerned about the lack of certainty
around access provisions for public authority access which are left to secondary
legislation.

**Scrutiny**

75. Under the draft Bill retrospective oversight of the new system of data retention
will continue to be provided by the Interception of Communications Commissioner,
the Commissioner will continue to be appointed by the Prime Minister with his annual
reports made to the Prime Minister.\(^\text{97}\) Notwithstanding the efforts of the present or
future Commissioners, a system of limited retrospective authorisation comes
nowhere close to providing effective scrutiny of a system which carries such huge
consequences for personal privacy, particularly when we have so little detail about
the resources and in particular the technical expertise available to the Commissioner.

76. It is not an offence under RIPA to unlawfully access communications data and
whilst an offence may be made out under section 55 of the *Data Protection Act* 1998,
the only available sanction is a fine.\(^\text{98}\) While Liberty does not usually support the
creation of new criminal offences given the excessive amounts of criminal law that
already exists, unlawful access to communications data should be an offence under
RIPA, with appropriate penalties. Whilst most people will never know whether or not
their data has been improperly retained or accessed, for those who do find out, the
main consequence for a public authority of accessing data without the appropriate
authorisation, for example, is the possibility of civil action being taken against them
under the HRA. However, the majority of actions taken under the HRA in respect of
the use of RIPA powers must be taken before the Investigatory Powers Tribunal
(IPT). The procedure operated by the IPT is far from adequate. It is under no duty to
hold oral hearings before which a person may be represented and even if it does
decide to hold a hearing (purely at its discretion) all of the Tribunal's proceedings,
including the oral hearings, must be conducted in private.\(^\text{99}\) RIPA itself provides that,
subject to any rules made by the IPT, the IPT can only notify the complainant

---

\(^{97}\) RIPA, ss 57 and 58.

\(^{98}\) Offence of knowingly or recklessly, without the consent of the data controller
(a) obtaining or disclosing personal data or the information contained in personal data, or
(b) procuring the disclosure to another person of the information contained in personal
data. Section 60 provides that successful prosecutions will result in a fine.

whether they have won or lost. Rules made in 2000 provide that if the IPT finds in the complainant’s favour the IPT must provide him or her with a summary of their determination, including findings of fact. Note, however, that this is merely a summary of the determination and if a complainant loses no reasons at all will be given. Most astoundingly, there is no right of appeal from the IPT. Section 67(8) of RIPA provides that rulings by the IPT are not subject to appeal and cannot be questioned in any court, unless the Secretary of State orders otherwise. Section 67(9) provides that it is the duty of the Secretary of State to make such orders in relation to most categories of proceedings and complaints, yet no such orders have yet been made. This is because despite most of section 67 being brought into force in October 2000, subsection 67(9) has never been brought into force. This effectively means that in most cases in which a person seeks to argue that a public authority has used unlawful surveillance against them, they are required to bring proceedings before the IPT, which must hold proceedings in secret, may not hold an oral hearing, will not give proper reasons for its findings and from which there is no right of appeal. This is arguably a breach of Article 6 of the HRA itself which requires a fair and public hearing, and the right under Article 13 of the ECHR to an effective remedy. These provisions should be overhauled as a matter of urgency in order to provide an appropriate mechanism for the independent determination of any complaints regarding the lawfulness a disclosure. How can the public have any confidence in a process which is held in secret, gives little or no reasons for its decisions and whose judgment cannot be brought into question in any court of law?

Conclusion

77. The Government claims these proposals will do nothing more than ‘maintain capability’: in reality the Coalition is proposing much more. For the first time private companies will be instructed to collect information on billions of communications made by their customers for no other reason than the authorities’ future demands for access. This amounts to mass, blanket, monitoring of the population paid for and facilitated by Government but outsourced to the private sector. This would represent a fundamental shift in the nature of our society turning a nation of citizens into a nation of suspects.

Rachel Robinson
Isabella Sankey

100 RIPA, s 68(4).