Draft Communications Data Bill

Written Evidence to the Joint Committee on the Draft Communications Data Bill

August 2012

For further information contact

Angela Patrick, Director of Human Rights Policy

email: apatrick@justice.org.uk tel: 020 7762 6415

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100

fax: 020 7329 5055 email: admin@justice.org.uk website: www.justice.org.uk

Executive Summary

Surveillance is a necessary activity in the fight against serious crime. When targeted, it can play a vital part in our national security. Unnecessary and excessive surveillance, however, destroys our privacy and blights our liberty.

The Draft Bill builds on the existing - and inadequate – regulatory provisions in Regulation of Investigatory Powers Act 2000 ('RIPA'). JUSTICE considers that the RIPA model is neither forward-looking nor human rights compliant.

The provisions in the Draft Bill propose a nationwide and blanket intrusion into the private life of every person in the UK using modern technology to communicate, to enhance their daily lives and support their freedom of expression. It would provide for the exponential expansion of the collection of information about how we use the internet, mobile telephones, landlines and the post to communicate with each other. The Information Commissioner has called this a step-change in the relationship between the State and the citizen. We agree.

The provisions in the Draft Bill are broad, vague and unjustified. No significant, new safeguards are offered. Importantly, we are yet to see clear evidence to support the Government's case that such expansion is necessary or appropriate.

Currently, around 500 public authorities are capable of accessing our communications data using existing surveillance powers. RIPA allows these public bodies to self-authorise access to our personal information. JUSTICE considers that this approach poses a significant threat to our personal privacy. Prior judicial authorisation for access to surveillance powers, including access to communications data should be the default in most circumstances. Fewer public authorities should be able to access this sensitive information about our private lives and access should be limited to those circumstances when surveillance is strictly necessary, principally, for the purposes of preventing and detecting serious offences.

Root-and-branch reform of our existing law on surveillance is needed to provide freedom from unreasonable suspicion and a modern surveillance framework for a digital age; not the further expansion of surveillance capability without truly effective safeguards against abuse.

(a) Introduction

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance access to justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists. Last year, we published *Freedom from Suspicion: Surveillance Reform for a Digital Age,* calling for the wholesale reform of the existing legal framework for surveillance, in the Regulation of Investigatory Powers Act 2000 ('RIPA').[1]

2. We welcome the opportunity to submit both written and oral evidence to the Joint Committee on the Draft Communications Data Bill ('the Joint Committee'). We regret that the Draft Communications Data Bill ('the Draft Bill') is severely lacking in detail and posed as a broad enabling power to arrange for the collection, retention and use of personal information, with very little detail provided on how these powers might be exercised in practice. This approach will significantly undermine the effectiveness of pre-legislative scrutiny by Parliament, commentators and the wider public.

(b) Background

3. The Communications Data Bill introduced in 2008 by the previous Government, would have, among other things, required communications service providers to give police and intelligence agencies unprecedented access to their networks for the purposes of facilitating interceptions and requesting data. It was withdrawn in the face of widespread opposition from JUSTICE and other civil liberties organisations, Parliamentarians and the public. The former Director of Public Prosecutions Sir Ken Macdonald QC, for instance, described those proposals as seeking to create 'an unimaginable hell-house of personal private information'.[2] In 2009, the Labour Government consulted on a series of proposals which would enable the Government to require private providers to collect communications data, again for the purposes of facilitating access to that data by public authorities. Again, in the face of opposition, these proposals were shelved.[3]

---

[1] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age,* Nov 2012. Hard copies of this report will be provided to members of the Joint Committee on request. Chapter 4, which considers communications data, is provided as an Annex to this submission. http://www.justice.org.uk/resources.php/305/freedom-from-suspicion Hererin, '*Freedom from Suspicion*'.

[2] See '*Private firm may track all email and calls*' by Richard Norton-Taylor and Alan Travis, The Guardian, 31 December 2008.

4. The Coalition Programme for Government committed to 'end the storage of internet and email records without good reason'.[4] Yet, early in its life, the Coalition also committed to 'introducing a programme' to revisit access to communications data.[5] However, the Government also promised to legislate in order to 'put in place the necessary regulations and safeguards' that would 'ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties'.[6]

5. Unfortunately, the Draft Bill fails to make good on these commitments to robust safeguards for the protection of our right to privacy online.

6. The Draft Bill builds upon our existing framework for surveillance in the Regulation of Investigatory Powers Act 2000 ('RIPA'). RIPA currently provides for requests for access to communications data. Communications data is defined by RIPA and includes subscriber data, traffic data and user data. Broadly, subscriber data is information held by a provider about a user; traffic data outlines information such as the location of the communication and the people involved, and details of the equipment used; and use data relates to the use made of the relevant service (for example, what websites a user has visited etc).[7] Named public bodies can access different categories of data for different purposes, following internal administrative authorisation by a senior officer within their organisation. Following the passage of the Protection of Freedoms Act 2012, local authorities may only access limited data following authorisation by a magistrate (although these provisions are not yet in force).

7. The request to a service provider may be in the form of an authorisation (section 22(3)) or a notice (section 22(4)), the difference being the former is a request for information that the provider already holds, while a notice is a direction to the provider to acquire it on behalf of the requesting body. Notices and authorisations last one month unless renewed.[8] Service providers must comply with notices requiring access to

---

[3] JUSTICE's submission to the Home Office Consultation, *Protecting the public in an changing communications environment,* in 2009 is available, here: http://www.justice.org.uk/resources.php/190/communications-data-collection-and-use-justice-response

[4] Cabinet Office, *The Coalition Programme for Government*, p11

[5] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44.

[6] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44.

[7] *Freedom from suspicion,* Chapter 4, provides fuller details on the existing rules governing interception of communications data. Sections 21 and 22, RIPA govern the current framework.

[8] Section 23(4) and (7).

communications data under RIPA, unless it is 'not reasonably practicable' to do so.[9] If necessary, the Secretary of State can seek an injunction for the enforcement of the notice.[10] Oversight is provided by the Interception of Communications Commissioner.[11] Since late 2005, public bodies able to make requests have been subject to an inspection regime carried out by an inspectorate under the direction of a Chief Inspector and the supervision of the Commissioner.

8. The Data Retention (EC Directive) Regulations 2009 (which implement the EU Data Retention Directive)[12] require certain public communications operators to retain information originally held for commercial purposes for up to 12 months.[13]

9. The overriding difference between the existing framework and the Draft Bill is the shift away from the presumption that for limited purposes, the State may access data already retained or reasonably obtainable by service providers, when shown to be necessary and proportionate for the prevention or detection of crime and other reasons which serve the public interest. While the existing measures are flawed (we return to this below); the Draft Bill would create a power for the Secretary of State to determine that all communications data about the population's activities and habits should be retained on a blanket basis, "just in case" it should prove justifiable for a public authority to seek to access that information. This potentially exponential expansion of the storage of data about our personal lives would create a new, and JUSTICE submits, inappropriate, understanding about the role of the State in private communications.

[9] Section 22(7).

[10] Section 22(8).

[11] Section 57(2)(b)). See further Chapter 3 above.

[12] Directive 2006/24 EC

[13] SI 859/2009

(c) The Draft Bill

10. Part 1 of the Draft Bill closely follows the intention of the previous Government by proposing that the generation, collection and retention of data about all online and telephonic communications in the UK becomes universal, with information about us all gathered and stored without any connection to the likelihood that our communications are connected with criminal behaviour.[14]

11. Clause 1 creates a broad delegated power which will allow the Secretary of State to compel "telecommunications operators" to generate, collect or otherwise obtain new data about our communications which is neither required by providers for commercial purposes nor currently held.[15] It makes clear that the requirements which can be imposed will be very broad, including to generate, collect, retain and process data; to comply with specific standards or to use specific systems (including through the development, acquisition and use of new software or hardware).

12. However, the detail of how these arrangements will be secured is left to secondary legislation and very little information is provided in either the Explanatory Notes or the accompanying impact assessments prepared by the Home Office. No Draft Order has been produced for consideration by the Committee. Detailed arrangements will be made by a combination of Order (by affirmative resolution) and subsequent notices served on individual providers (which may not be published or provided to parliament for scrutiny).[16] Given the seriousness of the change proposed by the Draft Bill, the limited information provided for the purposes of parliamentary and public scrutiny significantly limits the ability of both decision makers and commentators to closely examine how the technology and procedures envisaged by the Government will operate in practice.

---

[14] The previous proposals initially proposed a Government database for this purpose; early in the opposition to its intent those proposals shifted to focus on compulsion of private providers to gather information about their users for the purposes of ensuring that material should be available should it be requested by public authorities.

[15] Clause 1

[16] Clause 7(1) explains that notices served and provided for by any Order made under Clause 1 must be in writing and must specify the person to whom it applies and must be given in such a way as to draw it to that person's attention. There is no requirement for publication. It is clear that the Secretary of State would be empowered to publish but not required to do so. While providers might insist on a certain degree of commercial confidence, since a significant amount of detail about how our communications data will be retained and protected from inadvertent disclosure may be in such notices, it limits the opportunity for both parliamentary and public scrutiny significantly if even the general terms of how the technology and processes envisaged by the Bill will operate in practice. Similar notices served under existing powers – e.g. under the Data Retention Regulations – have not been published. When requests for publication have been made, they have been refused for reasons of "national security".

13. Part 2 of the Bill provides the regulatory regime for access to the data collected under Part 1. It broadly replicates the existing administrative procedures in RIPA, with the only prior judicial authorisation required by local authorities (Clause 11). All other public authorities will be able to access the data after self-authorisation following an administrative process set out in the Draft Bill (Clause 9). The list of public authorities empowered to access the data collected will be provided by Order (no draft has been provided, as the Secretary of State is reviewing whether existing authorities empowered to access communications data to continue to do so). At a high point, in 2007, 795 public bodies were eligible to access communications data under RIPA.[17] There remain over 500 bodies currently authorised under RIPA.[18]

14. Clause 14 of the Bill gives the Minister the power to establish 'filtering arrangements' for the purposes of 'facilitating the lawful, efficient and effective obtaining of communications data'. The Government has explained that the 'filtering mechanism' will be automated but will be able to search across different sources of data held by different providers to ensure the most effective answer to an individual public authority request for access to data. The Explanatory Notes make clear that the filtering mechanism may operate before a request has been formulated (that is, before an individual authority has determined that a request is necessary and proportionate).[19] The Government stresses that although this information will be processed by a Government controlled mechanism, it will be done automatically and will not allow the public authority in question to access data unless specifically authorised under Part 2. The Bill provides for the Secretary of State to delegate the operation of this filtering mechanism to another public authority. It is unclear how this filter will operate, its intended technical specifications or who its intended operator will be.

[17] *Freedom from Suspicion,* para 173.

[18] In his last report, the Interception of Communications Commissioner reported that 400 local authorities alone were eligible to access data (he inspected 71 of those bodies). He inspected a further 99 public authorities also authorised to act under RIPA for this purpose. See Annual Report of the Interception of Communications Commissioner 2011, HC 496.

[19] Explanatory Notes, paras 74 – 77.

(d) Privacy, communications and data

15. That each of the distinct acts of collection, retention and use of personal information is protected by our right to respect for private life, home and correspondence guaranteed by is trite.[20] The protection of private correspondence is guaranteed by international and European law, in both Article 8 of the European Convention on Human Rights and the equivalent provision of the European Charter of Fundamental Rights.[21] The collation, retention and use of personal information are specifically protected by the domestic and EU legal framework on data protection, for example in the Data Protection Act 1998.

16. The authority for both the extension of the collection of data (in Part 1 of the Bill) and the provisions for access to it (in Part 2) must be justified separately by reference to a legitimate aim and must be shown to be proportionate and necessary to meet that aim. To avoid violating the right to respect for privacy, the statutory provisions authorising both retention and access must be "in accordance with the law":

    a. Are the provisions in the Draft Bill sufficiently clear and precise to allow individuals to understand when their data will be retained, and in what circumstances it may be accessed by the State?

    b. Do the provisions address a legitimate aim, addressing the prevention and detection of crime or other significant public interests?

---

[20] In *Malone v UK* (1984) 7 EHRR 14, the Court considered the attachment of a 'meter check printer' to a telephone line for the purposes of recording the time calls were made, to whom and for how long. The Court considered that the collection of this information engaged the right to privacy, but in these circumstances could be justified by reference to the commercial need for a supplier of services to legitimately ensure a subscriber is charged correctly. This use was proportionate and justifiable. However, passing the information to the police without statutory authority and relevant safeguards against abuse was not. See, for example, paras 56 – 84. It is worth noting the gathering and collation of the information here is justified by the commercial need to retain information. The Draft Bill does not limit its effect to material already held by suppliers and operators, but will require the generation or retention of data not needed for any commercial purpose. The question of justification here goes to whether the generation or retention of this information can be justified for the purposes set out by the Home Office in connection with the potential for some communications to inform investigations and inquiries by public authorities. In *Amann v Switzerland* (2000) 30 EHRR 843, for example, the Court held that the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted. In *Rotaru v Romania* (2000) 8 BHRC 449, at para 43, the Court stressed that even 'public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities'.

[21] Article 7.

c. Has evidence been produced to show how the provisions in the Bill will benefit this aim, and to support the Government's case that the interference with individual privacy posed by the Bill would be proportionate to the benefit to be achieved?

d. Are the proposals the least restrictive means of achieving the aim in question and have alternatives been considered?

e. Are adequate and effective safeguards against abuse provided in the Bill?

17. We explain below why, in our view, each of the distinct parts of the Draft Bill pose a significant risk to the individual right to privacy. As explained in one of the leading cases, surveillance often occurs without the knowledge of the individual whose rights are in play. So, in most cases an individual will never know whether his information has been reviewed or what has been retained. Only in the limited circumstances when the information is used in a trial or when an authority acknowledges the surveillance that an individual may be able to challenge its propriety. In these circumstances, there is a significant obligation on the State to ensure that surveillance powers are closely drawn, safeguards appropriate and provision made for effective oversight:

> *[it is] unacceptable that the assurance of the enjoyment of a right … could be…removed by the simple fact that the person concerned is kept unaware of its violation..*[22]

18. The Court stressed that the justification of any surveillance measures places a significant burden on States to adopt the least intrusive measures possible:

> *[P]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.*[23]

19. JUSTICE strongly opposes the proposal in Part 1 of the Bill to expand the generation, collection and retention of communications data. We consider that the expansion of the

[22] (1978) 7 2 EHRR 214, paras 36, 41.

[23] Ibid, para 42. See also Para 49: *'The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism adopt whatever means they deem appropriate'.*

pool of data collected about our on and offline relationships with one another poses a significant risk to our privacy and ultimately, the Government has failed to provide evidence to support this extended provision for the capturing of data. Existing provisions under RIPA to access communications data are already extremely broad and the Government has failed to illustrate clearly why these powers are inadequate or why proposals of the breadth proposed in the Bill are justifiable.

20. The retention of data poses an interference with the right to privacy, both in its creation and in the risk that it may be accessed unlawfully or in error. As the Newton Committee reported in 2003, 'there are obvious risks to privacy in keeping information about individuals. The existence of data creates its own demand for access to it from a wide range of bodies for a variety of reasons, mostly unrelated to national security. It also creates the potential for abuse'.[24] We therefore consider that the existing pool of communications data liable to be retained should not be expanded unless a case of strict necessity can be made out.

21. The Government must illustrate why these measures are needed. We accept that technology is changing; as is the way we communicate with each other. However, simply because it may be possible for the State to gain access to a significantly greater pool of information about our private lives as a result of this shifting technological and social base does not mean that it necessarily should.

22. We regret that the ECHR memorandum and the Privacy Impact Statement prepared by the Home Office and the other material provided to the Joint Committee falls significantly short of providing parliamentarians and the public with adequate information on its case for reform. We are particularly concerned about a number of statements made by the Government:

    a. **Expansion, not maintenance:** We take issue with the repeated assertion in the consultation document and associated materials with the assertion that these proposals are needed because a "vital tool is disappearing" or that the provisions are necessary to ensure "communications data is available…in the future as it has been in the past".[25] This is compounded by the ECHR Memorandum which refers to the "reduction in the availability of communications data" that "will have serious

[24] Report of the Review of Privy Counsellors of the Anti-Terrorism Crime and Security Act 2001 (December 2003), para 398.

[25] Foreword, *Draft Communications Data Bill*, Theresa May.

consequences for the UK" and the need to "mitigate the reduction in capabilities caused by the decline in the availability of communications data".[26] This capability gap is not evidenced in any of the documents associated with the Draft Bill. The Impact Assessment asserts that 'increasingly police and others are unable to get access to communications data; some data is no longer retained…for business reasons; some [providers] offering services in this country are based overseas'.[27] There is little clarification of the circumstances when communications data which would previously available is no longer, nor any evidence provided of how this gap has impacted on the ability to prevent or detect crime. Neither is information given about the Government's predictions on the impact of changing technological capabilities. In other words, the government seeks to justify the expansion of its – already considerable – powers to require the retention of communication data on the basis of a series of predictions, each of which is questionable at best and speculative at worst.[28]

The motivation for this change is in the evolving way that we communicate with each other. There is no change or decrease in the capacity of the authorities to access existing data, as provided by RIPA (by issuing a notice under RIPA, a public authority can require a body to generate information not otherwise held or under an authorisation to provide data already stored). Instead, the real concern is that as we change our means of communicating, the potentially available pool of communications data is expanding. Much of the data that could be collected about how we relate to one another is not currently collected and it may be technically impossible for providers to do using their existing systems. Without any statutory compulsion or business need, there is no motivation for private providers to generate this data about their users' activities. This is explained more clearly in the Impact Assessment which accepts that the Government has considered two specific problems: (a) that certain types of data about our communications is not currently generated; and (b) that many new forms of technology are based overseas and third-party providers within the UK do not routinely store information about their users activities on these forums.

---

[26] Draft Communications Data Bill, page 100.

[27] Impact Assessment, page 3

[28] This reflects the last consultation on this issue undertaken by the previous Government on this issue. The JUSTICE response to that consultation is available here: http://www.justice.org.uk/resources.php/190/communications-data-collection-and-use-justice-response. See para 6.

The provisions in the Draft Bill are not designed to redress a reduction in capability. Instead they are designed to increase the ability of public authorities to access information about how we communicate by widening the pool of information that is held in the UK about our activities on and offline. Specifically, they will target our use of new technologies like Facebook or Gmail which are web-based and without any need to store information about users within the UK. It will also cover private communications networks, such as those run by Blackberry or internal communications networks operated by companies and other businesses.[29]

b. **State collection of personal information:** The Government has implied that, since the data retained under the Bill will be retained by private sector providers, the obligation on the State to justify the retention is less onerous. The Government's view is that the only obligation in play on the State in these circumstances may be a "positive" obligation to effectively regulate the activities of the private sector in order to secure the safe retention of the data, including by enforcing the existing legal framework.[30]

This is potentially misleading. The State has distinct positive obligations to regulate the processing of personal information by private individuals, in order to protect individual rights. However, the issues raised by the Bill are far removed from the questions raised by the mishandling of personal information gathered by the private sector; for example, a failure of the State to regulate the misuse of privately gathered CCTV footage. The Draft Bill would place a compulsory obligation on the private sector to retain information which it would not otherwise need nor want. It is this compulsory obligation to retain – an act of the State, not the private sector - which must be justified. It may assist, in these circumstances, to view the providers as agents acting on behalf of the Government for the purposes of collecting and retaining data. The first question must be whether the Government has produced sufficient evidence to justify the requirement to retain.

[29] The Telegraph, *Data Watchdog questions case for e-mail snooping,* 02 April 2012. The Information Commissioner's Office referred to the expansion of the collection of communications data as a "step-change in the relationship between the citizen and the State.

[30] Explanatory Notes, ECHR Memorandum, paras 10 - 15

The second, whether that retention is in practice accompanied by adequate and effective safeguards for the protection of private information.[31]

c. **What does 'data' mean?:** The Government explains its view that interception of the content of communications should be considered a more serious interference than the data associated with it. However, the historical distinction about the retention of communications data and the interception of communications is not necessarily feasible in the light of evolving technology. The information recorded by a phone meter in the early 1980s is nothing, when compared to what is today recorded digitally in respect of every mobile phone call, text message or internet session. 'Traffic data' for a phone call, for instance, includes not only the numbers of the caller and the called, the time, data and duration of the call, but also data showing the location of each party, whether the nearest telephone exchange or – increasingly – GPS data. Similarly, the traffic data associated with a single email message will typically include not only the data and time of the message, when it was sent and received, etc but also the sender's login name and IP address, from which can be gained a variety of information including, in certain cases, the particular computer used and its location. Traffic data from an internet session will include similar information as well as, for instance, the URLs of websites visited (e.g. www.justice.org.uk), and the time spent on each site. In addition to so-called 'traffic data', communications data also includes 'service use' data produced by service providers, e.g. itemised phone bills or internet records, and 'subscriber

[31] Draft Communications Data Bill, pages 96 – 99, paras 8 – 15. In this section of the memoranda, the Government relies on a series of cases which relate to the positive obligations of the State to act to protect one individual against the actions of another private individual by regulating their conduct by law, including through the criminal law. So, in *Botta v Italy,* the Italian Government had a positive obligation to enforce disability legislation against private providers to ensure access for the applicant; in *KU v Finland*, the inability to force the disclosure of the identity of the user of an internet service meant that the Government failed in its positive obligation to provide a form of redress and protection for a child whose identity had been abused online; and in *Von Hannover,* the State had an obligation to protect an individual's privacy against the publication of photographs taken in a public place by a private provider without consent. None of these cases are analogous to the proposals in the Bill and we urge the Committee to examine the evidence which the Government has provided to justify the need to compel private providers to generate, collate and retain data for its purposes closely. These cases have more in common with the cases where the Government has collated material but not necessarily used the material in practice or where it has conducted "strategic" surveillance (see for example, *Rotaru v Romania*, *Amman v Switzerland* and *Liberty v UK* (App No 58243/00, Judgment dated 1 July 2008). The Government refers to the case of *Malone v UK*, considered above, where the Court considered the collation of metering information for billing purposes legitimate and compatible with Article 8 ECHR. As explained, the collection of information for legitimate commercial reasons will involve distinct consideration to the proposal to require the private sector to retain material it would not otherwise retain for public purposes.

data'; i.e. the name and date of birth of the customer, their billing address, contact and payment details.

In this sense, the idea of communications data as being purely 'envelope data' is highly misleading: nobody writes their friend's credit card details on an envelope, still less their own. It should also be obvious that the unnecessary or disproportionate disclosure of details about a person's private communications can in some cases be every bit as damaging to that person's privacy as an actual interception of their communications, particularly when it reveals their location at a particular time and date or the fact of their contact with a specific person. Similarly, a review of a person's internet activities can allow an intimate picture to be built about their individual choices and personal history, including information about their health. Storing the sum of our annual communications data across multiple providers could create an extremely full picture of our personal preferences, activities and habits. The collation of this kind of data, accessible directly or across data sets through a filtering mechanism could have a serious impact on our right to respect for our private lives.

Others are more capable of commenting on the technological feasibility of dividing content and communications data, but JUSTICE understands that this is increasingly difficult. As a group of academics in the Information Systems and Innovation Group of the London School of Economics noted in their 2009 briefing on the government's Interception Modernisation Programme,[32] the distinction between so-called 'traffic data' relating to internet use, on the one hand, and the actual interception of the contents of a communication, on the other, is becoming increasingly blurred, particularly by the use of deep packet interception:[33]

d. **Does collecting data violate our privacy?:** The Government argues that the collection and retention of data requires a lesser degree of justification than use of data. We accept that the proportionality of individual measures will vary according to the seriousness of the interference concerned (and its potential impact) and the significance of the evidence that the measures utilised are necessary and proportionate to any legitimate aim. However, the documents

[32] LSE Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (June 2009).

[33] Professor Peter Sommer of the Information Systems and Innovation Group quoted in the LSE press release, 'Home Office internet surveillance proposals won't work says LSE study', 17 June 2009.

accompanying the Bill give very little weight, if any, to the proposed interference with individual privacy posed by the expanded retention of communications data. Importantly, although the Privacy Impact Assessment tackles the privacy implications of access under Part 2, and safeguards associated with retention, it makes no provision or assessment of the justification for the compulsory retention provisions in Part 1. Significantly, it fails to grapple with ongoing European challenges to the Data Retention Directive; the specific implications of the collection of data for particular groups of individuals; or any wider human rights considerations associated with the generation and collection of data:

i. These provisions will operate in addition to the existing Data Retention Regulations which provide for some providers to retain certain user data for up to 12 months. The Regulations further than required by the EU Data Retention Directive. The Draft Bill would go significantly further by creating a default assumption that all information about our communications with each other might be retained "just in case", on a rolling 12 month basis, ensuring that at any one time the State will have access to an annual history of our on and offline activities. A significant number of EU countries have refused to implement the EU Data Retention Directive; and its provisions, or associated implementing legislation, declared unconstitutional by judicial authorities in a number of countries, including Ireland, Belgium and Germany. The European Court of Justice is expected to consider the compatibility of the Directive and its implementation across Europe in more detail during the next year when it considers a case referred to it from Ireland (*Digital Rights Ireland*).[34] That the Government has chosen to press ahead with the expansion of our framework for the collection and retention of communications data while this uncertainty continues at a European level is surprising.

ii. That the Government fails to grapple with the privacy impact of the retention of communications data is disappointing; but it also neglects to consider the potential impact of Part 1 on particular groups. For example, the Bar Council has, in its evidence to the Joint Committee highlighted the

[34] See for example, *Digital Rights Ireland v The Minister for Justice and Others*, [2010] 2006/3785P. A fuller consideration of each of the challenges is provided by the European Commission in its report to the Council and the European Parliament on this issue: COM (2011) 225. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

specific problems which may result from the collation of information generated by individuals communicating with their legal representatives, by lawyers communicating with their clients or with lawyers communicating with each other about their cases.[35] In so far as it fails to effectively recognise the right to legal professional privilege, the existing RIPA framework is flawed. That this Draft Bill fails to recognise the potentially chilling effect that Part 1 could have on the confidence of clients in the secrecy of their communications with their legal advisers is worrying. Further, there are no specific exemptions provided from the scope of Part 1 at all. This could mean that individual legal firms could be required as telecommunications operators to comply with an individual notice to generate data. JUSTICE considers that this would clearly violate both the right to respect for private life and the right to due process. However, without a clear exemption, or any indication from the Government on how these particularly sensitive communications will be handled, it is difficult to be assured. Other groups are equally overlooked. Communications between Parliamentarians and lobby groups, between MPs and their constituents; the communication of journalists with their sources; and the activities of trade unions, protest groups and opposition parties will all be covered by Part 1.

iii. The internet is a vital modern resource for freedom of expression and freedom of assembly. The public reaction to the prospect that our internet use might be monitored through the retention of data about our use has been vehement. This has been replicated in other countries where increasingly draconian controls have been placed by the State on the conditions for its use (for example in other EU countries implementing the EU Data Retention Directive). That the Government has failed to grapple with the potentially chilling impact of these measures on ordinary users of these services is some cause for concern. The lack of public consultation before the Draft Bill was published is perhaps related to the Government's narrow view of its potential and perceived impact on individual users.

e. **What are the real crime fighting benefits?:** The Government's clearest assessment of the justification for retention is found in the Impact Assessment,

[35] http://www.barcouncil.org.uk/media-centre/news-and-press-releases/2012/august/bar-council-calls-for-'snoopers'-charter'-to-protect-legal-communications/

which sets out in broad assertions the business case for reform and the expected benefits of the change proposed. However, the information provided is exceptionally slim. Expected benefits of the changes proposed in the Draft Bill are assessed at £5.0 - £6.2 billion and are based upon:

'*an analysis of criminal behaviours by the Serious and Organised Crime Agency and an analysis of the future communications market based on OFCOM and other market sources.'*

The benefits are said to accrue from preventing tax fraud and facilitating the seizure of criminal assets. However, they also include benefits accrued from 'lives saved and children safeguarded' based on standard estimates by Home Office economists. Other benefits which cannot be monetised include drugs seized, successful murder convictions and the prevention of terrorism. Without further explanation it is extremely difficult to understand how these asserted benefits have been calculated. It is clear that further evidence has been produced by the Government and Parliamentarians may wish to ask for further information.

However, nowhere in the information provided by the Government is there a clear explanation of the Government's view that the blanket collection of all communications data without connection to any specific type of communication or to the likelihood that the communications may lead to evidence of criminality can be justified. This unfortunately reflects the approach of the previous Government to the blanket retention of DNA gathered from people arrested but not convicted. The potential usefulness of successful DNA matches was inappropriately taken as the starting point for justification, as here the usefulness of access to communications data is held out as the sole pillar to support Part 1 of the Bill. However, this is inadequate for the purposes of the imposition of a blanket rule of this type, which must be examined closely for clear justification that the data retained is no more than necessary and proportionate.[36] For example, the Government makes no estimate of what proportion of the data retained is likely to be used in connection with the prevention and detection of crime; nor does it give any indication of how many cases where communication data assisted in

[36] See for example, *Marper v UK* (2009) 48 EHRR 50. In that case, the Court explained that measures which operate without regard to individual impact and characteristics must be accompanied by clear justification and appropriate safeguards, concluding that the then arrangements for the indefinite retention of DNA samples taken from innocent people arrested but never convicted was disproportionate and in violation of Article 8 ECHR.

conviction, that conviction could not have been obtained by other means; similarly, no figures are provided for the projected increase in capacity to secure convictions following the expansion of the collection of communications data proposed by Part 1. The answers to at least some of these questions must have been prepared in order to secure the financial estimates given in the Impact Assessment. However, they have not yet been disclosed.

f. **Striking the right balance?** JUSTICE considers that it is clear that the proportionality of these measures have not yet been fully explored by Government. The Government has not, satisfied the requirement for compelling evidence that these measures are strictly necessary. In our view, it is clear that they are likely to violate the right to respect for private life.

(e) The relevance of safeguards

23. The Government relies predominantly on proposed 'safeguards' against the arbitrary abuse of the new powers to support its case for reform. The case-law from Strasbourg on surveillance has focused closely on the efficacy of safeguards associated with surveillance in their examination of local laws for the protection of the national interest. As an international court, it has generally afforded a significant margin of appreciation to States in connection with State surveillance in assessing the necessity for particular measures. [37]

24. However, there can be no question that it is for Parliament to be satisfied that these intrusive measures are truly necessary and appropriate before proceeding with the proposals in the Draft Bill. Safeguards alone cannot justify the shift in the relationship between the State and the individual envisaged.

The generation, collection and retention of new data (Part 1)

25. The safeguards outlined by the Government in connection with the expanded collection and retention of communications data are themselves limited:

    a. **Retention is limited to 12 months**. The Government explains its view that the data retained will be destroyed after 12 months (except where extended for the purposes of legal proceedings) is a significant safeguard against abuse.[38] However, this safeguard should not be overplayed. While data will only be retained for a year, the effect of Part 1 will be to create at any point in time an annual picture of the population's communications activity. This rolling diary of communications data could be kept for each individual in the country, albeit stored across multiple providers and accessed through the Government controlled filter mechanism.

    b. **Use and processing limited:** The Government also points to the express responsibility on providers to destroy the data when it is no longer lawfully held

[37] *Freedom from Suspicion,* Chapter 2.

[38] Draft Communications Data Bill, ECHR Memorandum, para 14

and that use of the data other than authorised by the Draft Bill will be prohibited.[39] However:

i. This fails to acknowledge the significant number of public bodies who are already capable of accessing communications data for an extremely broad range of purposes (we return to this issue, below);
ii. It also neglects that the larger the pool of data collated, the greater the risk that it may be mismanaged or disclosed in error. In his latest report, the Interception of Communications Commissioner refers to almost 900 self reported errors under the existing framework for access. A failure to understand the scope of the powers in the Draft Bill could lead to unlawful disclosure. However, human and mechanical error can equally lead to the unlawful disclosure of data. Both private and public bodies have, over the past five years, suffered from significant embarrassment as a result of lost data (for example the Department for Work and Pensions losing information about families claiming child benefit).
iii. The Draft Bill and its Explanatory Notes make clear that not only will access be permitted for the purposes specified in the Bill, but for other 'lawful purposes'. The Government have explained that this could include a Court Order.[40] So, for example, disclosure might be sought in the course of civil litigation from a telecommunications provider through the use of a *Norwich Pharmacal* Order, for example, where one party to litigation argues that the provider is 'mixed up' in the dealings of the other party as a result of the use of his service for wrongdoing.
iv. The Draft Bill provides for the Secretary of State to expand the purposes for which access is permitted by Order (we return to this below);
v. The Draft Bill does not propose to create an offence of unlawfully disclosing data. If material is disclosed other than in accordance with the Draft Bill, it is likely that the most significant deterrent will be a fine imposed under the Data Protection Act 1998. In light of the fact that these requirements may be applied to businesses with a multi-million pound turnover, a fine may not be a significant deterrent. While we are reluctant to recommend new offences, but the limited deterrent of the existing

[39] Ibid

[40] Clause 5. Explanatory Notes, paras 30 – 31.

measures reduce the limits placed on individuals subject to Part 1 requirements.

c. **'Security obligations':** The Bill requires persons retaining data subject to Part 1 to put in place adequate security systems to govern access to the data and to protect against unlawful disclosure. Unfortunately, without further information about the technical and procedural arrangements imposed by Part 1, and the corresponding need for security, it is extremely difficult to assess the likely capabilities of any security arrangements. Since these specifics are likely to be confined to notices served on persons under Part 1, which may not be published, independent and impartial assessment of the effectiveness of security arrangements is likely to be impossible.

d. **Consultation and procedural guarantees**: Clause 2 of the Bill provides that when a notice is imposed, the Secretary of State must comply with certain consultation and procedural requirements. Unfortunately, these measures are entirely geared towards the protection of the interests of the persons subject to Part 1 notices, not the privacy rights of users. It provides for consultation with the person subject to requirements, with the Technical Advisory Board established under RIPA and OFCOM, none of whom have any specific obligation to consider privacy or the necessity and proportionality of the requirements being considered. We consider that while this would be a vital procedural requirement for the protection of the commercial and other interests of telecommunications operators, it adds little to the protection for individual users. There is no statutory requirement for public consultation proposed, nor is it proposed that the Information Commissioner's Office would be consulted.

e. **The role of the Information Commissioner's Office:** Part 3 of the Bill provides a new role for the Information Commissioner in relation to data held under Part 1. The Commissioner is required to keep under review the operation of measures relating to data security; the destruction of data and any provision in any Clause 1 Order which relate to data security (Clause 22(5)). While we welcome the recognition of a role for the Information Commissioner, we note that the proposed duties echo and supplement existing statutory functions which exist under the Data Protection Act 1998. While specific statutory functions here provide a degree of specific scrutiny, these are in themselves limited to data security. The Information Commissioner is not empowered to consider the necessity or

proportionality of any specific requirement or any issues relating to access by a public authority to data. These functions are reserved to the Interception of Communications Commissioner. In any event, the Information Commissioner has himself questioned whether without significant further resources he would be capable of conducting the review proposed in the Draft Bill.

f. **The role of the Interception of Communications Commissioner:** We consider that the oversight of the Interception of Communications Commissioner ('ICC') under the existing RIPA procedures is inadequate to protect the individual right to privacy. The provisions in the Draft Bill extend the existing measures to the new proposals in Parts 1 and 2 with little or no modification. We address the work of the ICC below.

Access to data (Part 2)

26. That the provisions in Part 2 broadly replicate the provisions in RIPA for access to communications data is disappointing. JUSTICE considers that there are a significant number of flaws within RIPA which are magnified when applied to the proposed expansion of data generation in Part 1. Principally, we are concerned that these powers will continue to be exercised by a far greater range of bodies than may be strictly justified and for purposes which are not necessarily proportionate in light of the impact of compulsory surveillance powers on individual privacy. As explained above, the bodies which will exercise the right to access data under the Draft Bill have not yet been finalised.

27. The purposes which trigger the right to access data gathered under Part 1 broadly follow those outlined in RIPA. JUSTICE considers that the purposes outlined in RIPA are already overly broad. Measures designed as compulsory powers for surveillance by the State may be essential for the investigation of serious crime, but as the purposes in RIPA devolve from the prevention and detection of serious offences the risk that they will be used disproportionately increases. When RIPA was introduced, the only bodies to exercise powers under the Act were the police, intelligence services and HMRC. While the powers under the Act might appropriately be extended to other law enforcement agencies and the emergency services, its extension to other bodies should be justified by reference to the strict necessity test identified by the Strasbourg Court. When these powers are extended to the investigation of minor criminal or regulatory offences such as fly-tipping, or for administrative purposes, such as the checking of school catchment, we

consider that their use is highly likely to be disproportionate. That is not to say that such minor offences are not important or deserving of investigation. Rather it is that the harm involved is by definition insufficiently serious to justify the inherent risk that surveillance poses to the privacy of any person under suspicion. Similarly, in connection with the use of these powers for other purposes (such as the identification of persons), less intrusive forms of investigation are likely to be an equally effective and therefore more proportionate means of investigating minor crimes than the resort to surveillance powers.[41]

28. In addition, many of the safeguards relied upon by the Government are also based upon the flawed procedural arrangements of RIPA:

    a. **Authorisation:** JUSTICE considers that the administrative authorisation procedure provided for in Clauses 9 and 10 provide for inadequate independent scrutiny of the need for access to data. These provisions are largely modelled on RIPA. In *Freedom from Suspicion,* we explained our view that prior judicial approval should be the default authorisation mechanism for most surveillance activities, including access to communications data. While it is no doubt true that senior members of organisations are typically well-placed to supervise the operational decisions of their subordinates, and more mindful of their ultimate accountability to the public, it is also clear that senior and junior members of the same organisation will inevitably share an interest in achieving the necessary results. The relative seniority of a Police Superintendent would not normally be enough, for instance, to make her sufficiently objective to authorise a search warrant, unless it was a genuine emergency and there was not sufficient time to approach a judge. Still less is it realistic to expect a Deputy Chief Inspector to be sufficiently independent of an investigation being carried out by his subordinates in the Trading Standards Service, for example, to objectively assess whether secretly accessing someone's communications data is a necessary and proportionate interference with their right to privacy.[42]

[41] *Freedom from Suspicion,* paras 180 – 181.

[42] See e.g. LSE Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (June 2009), p30: 'now seems a good time to question whether a senior official in an organisation with an interest in the outcome of an investigation is the best person to judge the application for access to communications data made by a junior figure in the same organisation'.

Although the Courts have stopped short of expressly requiring prior judicial authorisation in all cases, in many cases it has been considered essential. It is seen as the paramount means of protecting individual privacy in instances where the individual themselves may be unaware that their information is being handled. In those cases where no form of prior judicial oversight has been available the other safeguards imposed by domestic arrangements for surveillance have been robust and scrutinised extremely closely and the measures in question have been subject to robust review after the event.[43] For example, in a recent decision involving retention of information about a student, the Court said:

> *The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.* [44]

b. Proportionality and necessity: The requirement in the Bill that only authorisations which are proportionate and necessary should be a significant safeguard against abuse. The Bill requires that the measures in question be proportionate to the goal to be achieved. Since access engages privacy, this requires public authorities to effectively apply the Convention test set out above to each access authorisation. Unfortunately, in practice, the application of this restriction in RIPA has not proved a significant barrier to access. Neither public authorities, individual officers or the Interception of Communications Commissioner appear to have applied a rigorous review of the proportionality of existing requests from a human rights perspective.

For example, in the context of restricting access of local authorities to communication data, the Interception of Communications Commissioner considered existing powers exercised proportionately as requests from local authorities made up a low proportion of overall requests and there had been very few errors self-identified by local authorities. He also considered the use of RIPA for the purposes of pursuing fly-tipping an appropriate and proportionate use of

[43] See for example, *Uzun v Germany*, App No 35623/05, 2 September 2010.

[44] *Rotaru v Romania* (2000) 8 BHRC 43 at para 59.

compulsory surveillance powers, regardless of other means of investigation.[45] He failed to consider whether the use of the powers in individual cases had been justified. Similarly, during the Joint Committee's evidence on the Draft Bill, it has been suggested that the police use these powers for "non-crime" purposes and for low level traffic offences.

There is, an inherent risk in any criminal investigation involving intrusive surveillance that the resulting invasion of privacy will in hindsight prove to have been unnecessary because the initial suspicion turns out to be false: what Lord Neuberger described as one of the paradoxes of surveillance.[46] This inherent risk can be minimised by, for example, requiring that less intrusive means be considered first, but it can never be eliminated.

Whether it is proportionate, therefore, to run the risk of invading someone's privacy in the knowledge that they may turn out to be innocent depends on several factors, including the reasonableness of the suspicion *but also* the seriousness of the offence in question. It is the difference, in other words, between breaking down the door to someone's hotel room because you think they are being murdered, and breaking down to door to their hotel room because you think they have stolen your toothbrush. In both cases, your suspicion may be very well-founded but there is also an inevitable risk that you are mistaken. And should it turn out that you are mistaken, the reasonableness of your suspicion will be of little comfort to the person whose privacy you have unnecessarily invaded. But at least in the case of suspected murder, we would say that the seriousness of the suspected offence, combined with the reasonableness of your suspicion helped to excuse your actions. The same could not be said of the toothbrush.[47]

Unfortunately, there is little evidence that this test is being applied appropriately in practice or that it operates as a significant safeguard for personal privacy.

c. **The role of the Interception of Communications Commissioner and the Investigatory Powers Tribunal:** The role of the Interception of Communications

[45] *Freedom from Suspicion,* paras 172 – 181.

[46] *In re McE* [2009] UKHL 15 at para 111.

[47] For further information about the application of the proportionality test in this context see: *Freedom from Suspicion,* paras 172 – 181.

Commissioner and the Investigatory Powers Tribunal is not capable of providing adequate, independent and transparent review to provide reassurance that individual privacy is respected in the operation of RIPA. As explained above, ex-post judicial review may be adequate in order to ensure respect for private life only where that review is accompanied by adequate existing safeguards to ensure that individual rights are afforded appropriate respect. Unfortunately, review by the ICC and the IPT is significantly lacking. Both mechanisms are fundamentally flawed. As we explain in *Freedom from suspicion*:

i. Review by the ICC is by way of 'dip-sample' and the self-reporting of errors. This means that only a handful of the almost 500,000 requests for communications data a year are reviewed (for example, there were 895 individual errors self-reported to the Commissioners office during the last reporting period; and he inspected less than 200 individual public authorities exercising powers in connection with communications data);

ii. Between 2005 and 2010, no reports were made that any public authority decision had been disproportionate or unnecessary. In 2011, the Commissioner reported that in one case it had been reported that powers had been used inappropriately. However, this latter case involved use of communications data powers in connection with school admissions, an issue which had been considered by the IPT in the *Paton* case and held disproportionate (and which had been covered significantly in the press during 2011). As the Commissioner highlights in his report, this is the only case in which his inspections have identified an inappropriate use of these powers.[48] Given that there have been probably somewhere close to three million requests made since January 2004, this suggests either a degree of effectiveness in public body decision-making that approaches infallibility, or more likely, that the Commissioner's oversight is ineffective.

iii. The IPT lacks transparency and any of the procedural safeguards associated with accessible redress or effective oversight offered by ordinary tribunals. The likelihood that individuals will become aware of surveillance is low (in the *Paton* case, the surveillance came to light due an error made by a local authority employee), making bringing a case before the IPT extremely unlikely. When cases are brought, they may be

[48] 2011 Annual Report of the Interception of Communications Commissioner HC 496, page 44.

argued in secret, and in the absence of the applicant and their legal team. If a case proceeds to a decision by the Tribunal, the applicant may only be told if he has won or lost and may be significantly deprived of any reason for the decision in the case.[49]

d. Filtering: The Government refers to the filtering arrangements in the Draft Bill as "minimising" the likely interference with Article 8 rights posed by requests for access.[50] As explained above, we find this argument extremely difficult to follow. There is very little information available about how the filtering mechanism will operate. However, what has been explained is that this mechanism will allow the Government to "join up" data sets held by numerous providers to provide a fuller picture relevant to a request. This mechanism will enable the creation of an extremely full picture about an individual's private life – or the activities of a group of individuals. This information will be accessed before a request is authorised, albeit within the filtering process. This in itself would appear to create a greater risk to individual privacy, not an additional safeguard. Without significant further details on the technical and procedural arrangements for the operation of the filter, including which public authority will operate it, it is impossible to provide a reliable and clear analysis of the risks associated with its functioning.

e. Repeal of General Powers: The ECHR Memorandum and the Privacy Impact Assessment includes the decision to repeal certain general powers to access data within the Government's assessment of the proportionality of these measures.[51] JUSTICE have called for the repeal of these general powers, which would most likely fail any Convention challenge if one were brought, for lack of legal certainty or appropriate safeguards. The Government committed in its counter-terror review published in January 2011 to rationalise the bases by which communications data could be acquired.[52] We welcome the decision to repeal these provisions. However, this decision should not be treated as a trade-off or a *quid pro quo* for the expansion of data collected.

---

[49] A fuller critique of the ineffectiveness of the IPT is provided in *Freedom from Suspicion,* at Chapter 9.

[50] Explantory Memorandum, para 21

[51] Explanatory Memorandum, para 21.

[52] Cm 8004, January 2011, page 5.

(f) Time to rip up RIPA?

29. The introduction of the Draft Communications Data Bill provides an ideal opportunity for Parliament to consider the underlying legal framework for the existing broad powers of state surveillance in RIPA. The existing pool of communications data liable to be retained should not be expanded. Instead, RIPA should be revisited with a view to significant reform. In so far as access to communications data is concerned:
    a. **Public authorities:** The number of public authorities able to access communications data should be significantly reduced; and ideally limited to the police, law enforcement agencies intelligence and emergency services and to any other bodies dealing with serious criminal offences;
    b. **Access:** The purposes for which communications data may be accessed should also be revised, with a view to limiting significantly the circumstances when communications data may be used proportionately. While the requirement that the measures should only be exercised when necessary and proportionate should be a significant limitation on the circumstances when data requests are made; in practice this has not operated as a particular restriction to administrative authorisation;
    c. **Prior judicial authorisation:** The default for the majority of requests should be prior judicial authorisation. This will significantly increase the independence of the oversight mechanisms in play and the likelihood that data will only be accessed when necessary and proportionate. Exemptions may be considered to allow police, law enforcement agencies, intelligence and emergency services access to limited subscriber data (including information about account holder's name, address and contact details, for example) and for access in emergency situations to other data (subject to a subsequent judicial authorisation within a reasonable period, for example, 48 hours).[53] Some objection has been raised about the use of prior judicial authorisation in connection with administrative difficulties, the need

[53] An exception based on ad-hoc supervision could be carved out for law enforcement bodies acting in an emergency (as explained above and in *Freedom from Suspicion*). The bulk of requests for communications data relate to requests from the police, law enforcement and other agencies for subscriber data. (Between 2005 – 2011, the proportion of requests has been between 54% and 80%. See *Freedom from suspicion,* para 160. See also 2011 Report of the Interception of Communications Commissioner.) Access to limited subscriber data (such as name, address and contact details) by the police and other law enforcement agencies or emergency services might justifiably be exempted and subject to administrative authorisation. However, we note that although the definition of subscriber data used in the Bill reflects the provision in RIPA, the application of that definition to the new proposals to gather data in Part 1 will expand its effect (for example, subscriber data might include a Facebook profile, information held by a university network about its students, including for example, transcripts, or by employers about their employees). We would consider prior judicial authorisation as a default the appropriate trigger for access to this kind of data.

for speed and costs. We consider that these difficulties should not be overplayed, particularly in light of the breadth of the powers being exercised and their implications for personal privacy.

d. **Review and oversight:** If prior judicial authorisation is in place as a default, the importance of subsequent review will be less significant and less onerous. However, we have recognised that independent monitoring and review of decisions made and the operation of the legislation would be sensible. In our view, this should be conducted by the Information Commissioner in connection with non-law enforcement activities and by the Surveillance Commissioners in so far as review is necessary in connection with the activities of the police, law enforcement and intelligence agencies.[54]

(h) Conclusion

30. These proposals have been presented by Government as an innocuous and technical shift necessitated by degradation in existing investigatory powers. Instead, the Draft Bill creates a platform for the Government to collate information about each of us which would allow an undefined list of public authorities access to a rolling annual diary of our on and offline personal lives for an extremely broad range of purposes. This would be a step-change in the way information about our conduct is stored, being collated "just in case" it may be useful for State purposes.

31. We urge the Joint Committee to reject the Government's case for reform and to call for renewed focus on the failings of our existing law on surveillance before further legislative expansion of the collection of personal data is pursued.

JUSTICE

August 2012

[54] Further, more detailed information about JUSTICE's recommendations for reform can be found in *Freedom from Suspicion,* at pages 85 -86. See Annex 2

Annex – Call for Evidence: The Committee's Questions

In our written evidence, we have focused on our key concerns about the Bill.

We provide below short summary responses to a number of the questions issued by the Committee, for ease of reference. These summary responses should be read together with our full submission and paragraph numbers are provided for cross-reference. That we have not provided an answer to one of the Committee's questions should not be read as support for any part of the Bill.

GENERAL:

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

- JUSTICE does not consider that the Government has made a convincing case for reform. The powers provided for in the Draft Bill are extremely broad and the justification provided is entirely lacking in evidential support. They supplement an already broad legal framework for surveillance in RIPA, which in our view, lacks the essential substantive and procedural safeguards necessary for the protection of individual privacy.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

- The proposals in the Draft Bill would create a blanket authority for generation and collection of unprecedented amounts of information about how we all communicate in the UK, whether on or offline. We consider that its provisions pose a serious risk to our right to respect for privacy.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

- These provisions will operate in addition to the existing EU Data Retention Regulations which provide for some providers to retain certain user data for up to 12 months. The Regulations go far further than required by the EU Data Retention Directive. The Draft Bill would go significantly further by creating a default assumption that all information about our communications with each other might be retained "just in case", on a rolling 12 month basis, ensuring that at any one time the State will have access to an annual history of our on and offline activities.

- A significant number of EU countries have refused to implement the EU Data Retention Directive and its provisions, or associated implementing legislation, declared unconstitutional by judicial authorities in a number of countries, including Ireland, Belgium and Germany. The European Court of Justice is expected to consider the compatibility of the Directive and its implementation across Europe in more detail during the next year when it considers a case referred to it from Ireland (*Digital Rights Ireland*). That the Government has chosen to press ahead with the expansion of our framework for the collection and retention of communications data while this uncertainty continues at a European level is surprising.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

- As explained above, the legality of the provisions in the EU Data Retention Directive is subject to review. JUSTICE has commissioned further research on the relevance of the EU Framework for the debate on the Bill. If this is available while the Joint Committee's inquiry is ongoing, we will provide it to members.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

- We consider that these measures pose a significant risk that they will violate the individual right to respect for privacy in practice. Rights cannot be swopped like trading cards. If interference is identified, the only way of addressing the violation concerned is to remove the interference or to adopt additional safeguards to reduce its impact. Removing unrelated but offending measures cannot provide redress.

- That the Government's Memorandum on the ECHR and the Explanatory Notes accompanying the Bill present the repeal of a number of general powers for public authorities to obtain information as a "quid quo pro" for the provisions in the Bill or an additional safeguard for personal privacy is inappropriate. Each of these ill-defined general powers were liable to challenge regardless of the introduction of the new measures in the Bill.

  While their repeal is welcome, this should not be treated as a "trade-off" for the equally ill-defined and contentious powers in the Draft Bill.

SCOPE:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

- The number of public authorities currently able to use surveillance powers under RIPA has expanded exponentially. We consider that the number of bodies capable of using surveillance powers more generally is disproportionate. Equally we are concerned that the use of surveillance powers disproportionately in connection with administrative or regulatory offences and minor crimes is inappropriate and consider that the purposes for which surveillance powers might be used should be revisited.

- The Secretary of State seeks the flexibility of a discretion to expand the scope of the powers in the Draft Bill, arguing that the repeal of general powers may require the expansion of the scope of the Draft Bill as bodies make a business case for the use of the powers therein.

  JUSTICE considers that many of the general powers are ripe for repeal and that alternative means of pursuing the functions they were determined to serve are available without resort to surveillance. That the necessity for the use of these powers has not been explored at this stage is a cause for concern, not justification to

provide the Secretary of State with a delegated power to revisit the list of bodies which are able to access our communications data.

USE OF COMMUNICATIONS DATA:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

We consider that the existing provision for access to communications data should be reviewed, with a view to restricting the number of public bodies who can use these powers. Ideally the powers should be used principally for the prevention and detection of serious crimes and by bodies with functions designed for that purpose.

SAFEGUARDS:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

We consider that the existing framework for access to communications data should be amended to provide for prior judicial authorisation as a default in most cases. We consider that the oversight offered by the Interception of Communications Commissioner does not provide adequate scrutiny to protect the individual right to respect for privacy.

PARLIAMENTARY OVERSIGHT:

32. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

- We consider that there is very limited provision for parliamentary oversight in the Draft Bill. The Draft Bill and its accompanying documents provide little detail on how the measures proposed will work in practice, including how safeguards will be formulated. The Committee has not been provided with any Draft Order which would provide a fuller picture of how the Government proposes to proceed.

- The Draft Bill would achieve its goal by a combination of Order (affirmative resolution) and notices (governed by the Order and not necessarily published). We consider that the lack of detail about the proposed Orders, and the lack of transparency which will

operate in the notice scheme significantly limits the opportunity for effective parliamentary scrutiny of the impact of these measures on the right to privacy in practice.

TECHNICAL:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

23. How safely can communications data be stored?

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

- These questions are best addressed by others with greater technological expertise. However, there is limited information available on the technology which the Government intends to use, and it is clear that it is expected to vary according to the arrangements in place with each provider or operator. This information will likely be included in notices which may never be published and the opportunity for independent scrutiny of the effectiveness of the technology utilised will be extremely limited

- Storage of personal data by the public and private sector is notoriously difficult. Errors have occurred in both human and automated systems which have led to the inadvertent disclosure of information unlawfully.

- As we explain above, we regret that the filtering arrangements provided for in the Bill are far from clear or appropriate.

Annex 2

Freedom from Suspicion: Chapter 4