Open Rights Group Submission
to the draft Communications Data Bill Joint Committee

August 2012

Contents:

For more information contact Peter Bradwell, peter@openrightsgroup.org

Introduction

1. We believe the powers contained in the draft Communications Data Bill are too broad and will result in a generalised surveillance of the population. Law enforcement access to communications data for specific purposes is not wrong in principle. But we do not believe the generalised collection of communications data about the population by the government and law enforcement bodies is acceptable in a liberal democracy.

2. Where incursions into the public's private lives are proposed, and justified with reference to competing rights such as security, the benefits case must be made openly and trade-offs must be established via a clear and robust democratic process. We are concerned the Joint Committee is being asked to make recommendations based on incomplete or inaccurate information.

3. In this submission we argue that there has not been sufficient opportunity for the public or Parliamentarians to properly scrutinise the proposals. We set out concerns about the scope of the information likely to be collected and the safeguards governing access to it. Quite clearly this Bill amounts to more than a proposal to maintain existing powers. Too much information will be collected about too many people.

4. We argue that 'new' kinds of communications data, from social media for example, are simply not comparable to phone record data. They can be far more intrusive and revealing and, of course, far more useful. This is especially so when data is combined to create a broader picture of an individual's movements, personality and social circles. So we refute the suggestion that communications data does not somehow convey substantive content about a person's life. We believe that the term 'communications data' is being stretched to breaking point, and can not adequately contain the variously intrusive and revealing types of data now potentially available to law enforcement. It has reached its limit as the useful basis for a single regime of information storage and access.

5. We set out why we believe the proposed safeguards around access to communications data are too weak, which will result in both the accidental and deliberate misuse of the data leading to significant privacy harms. That will likely include risks to journalists and their sources, the undermining of legal privilege and a chilling effect on whistleblowers. We also note how information provided by the Interception of Communications Commissioner about the error rate in RIPA requests seems to be based on a flawed reporting process, and there is insufficient data to make informed, independent analysis of the regime.

6. We recommend the current draft Bill is rejected. We suggest there are alternatives to these proposals that would involve less intrusive and harmful powers but which have seemingly not been considered, for example a form of properly managed directed (rather than general) collection, with court approval for access, in cases where suspicion exists. We suggest a more detailed, and public, consideration of the various types of information potentially available to law enforcement, how useful and intrusive that information may be, and what collection, storage and access regimes are appropriate.

7. We include in our submission a legal opinion from Eric Metcalfe of Monckton Chambers, former director of JUSTICE, in which he considers the consistency of the draft Communications Bill with human rights law (Annex A). He concludes that the Bill is incompatible with the UK's obligations under Article 8 of the European Convention on Human Rights. The full opinion is attached to this submission. We also include in Annex B evidence from Public Concern at Work, detailing case studies of recent threats to whistleblowers.

Summary of key points

- We recommend that the draft Bill as it is written is rejected. The powers to order the collection and storage of information are too broad, and the safeguards over access are too weak.
- The Government has not run an adequate policy making process. The proposals seem built to *withstand* public scrutiny and debate rather than be subject to and improved by it. There has been no consultation and they have not provided sufficient detail regarding how the powers will work in practice, nor the associated costs and benefits. We recommend a full review of, and consultation on, communications data collection and access.
- The powers amount to a general surveillance of the population. We recommend an analysis of how a properly regulated regime of targeted collection would be more appropriate.
- Drawing on the attached legal opinion, we consider the proposals to be incompatible with the UK's obligations under Article 8 of the European Convention on Human Rights.
- We recommend court approval for all access to communications data.
- We recommend a system of notification for people whose data is accessed.

Issues with the policy making process

8. We welcome the scrutiny that the Joint Committee has given the draft Bill thus far. We also believe that the lack of a full public consultation and the paucity of detail available to the public and the Committee have undermined the policy making process and led to an inadequate public debate.

9. The government have not 'built in' to this process an opportunity for a democratic debate about a broader range of options for addressing the 'capabilities gap' identified by the Home Office.

10. The proposals and the process that led to their creation appear to have been built to avoid and withstand public scrutiny, rather than to be subjected to and improved by it.

The lack of detail

11. Part 1 of the Bill sets out extremely broad powers. As a result, it has been difficult to establish with any clarity how collection and storage of information will work in practice.

12. For example, there is no detail on what the orders may look like. On 9th July both Rt Hon Simon Hughes MP and Dr Julian Huppert MP asked for more detail on the orders that may be written under the powers of the Bill[1]. It is fair to say the answers were not comprehensive:

> **Simon Hughes:** I am grateful to the Minister for his answer. He will know that the draft Bill, particularly in clause 1, gives very wide powers to the Secretary of State by order. Will he tell us whether the Secretary of State has yet written those orders? In any event, will he give the undertaking that they will be published at the earliest available date?
>
> **James Brokenshire:** It is worth underlining that communications data are an essential tool in solving and prosecuting crime. It is important that that is not eroded by changing technologies, which is why we need the flexibility to respond to change. We are working closely with the Joint Committee. We are absolutely committed to the pre-legislative scrutiny and to ensuring that the Committee can conduct robust scrutiny of the Bill.
>
> **Dr Julian Huppert (Cambridge) (LD):** The Minister said that he was working with the Joint Committee on which I serve. He will be aware that the Joint Committee has not been given sight of the order. Will he promise that we will have a chance to see it while we are carrying out the pre-legislative scrutiny?
>
> **James Brokenshire:** As my hon. Friend will know, scrutiny of the draft legislation is only just starting. I understand that the first sitting of the Joint Committee is due to take place this week. Officials from the Department will consider this matter and give evidence to the Committee. I will commit to keeping the issue under review as the legislative process develops, because we recognise the need to ensure that the Bill and the scrutiny that we will respond to are effective. We need to recognise that this is an important matter in ensuring that crimes continue to be prosecuted.

13. We are not aware of the Joint Committee receiving further detail along these lines, nor are we aware of the Home Office releasing such details publicly. As a result, it is difficult to examine in great detail exactly what the Home Office have in mind.

14. One consequence of this is that the Home Office has focused simply on whether communications data is useful in principle, or whether using communications data to solve crime is a good idea. Communications data is obviously extremely powerful and useful data. The important debate is about the types of information potentially available, the means of collecting and storing it, the relative levels of intrusiveness and usefulness and the suitable regimes for access to it. The decision making process focused on that should take place through democratic fora involving a public consultation.

15. These proposals have been presented as *the* possible option for addressing the issue of access to new types of 'communications data'. In her introduction to the draft Bill, the Home Secretary begins by telling a story of the capability gap and why closing it is vital to maintaining the ability of law enforcement to deal with serious crime. However, absent from the introduction is a consideration of what information is and is not available, to whom, the power of that information and any possible harms that may come about from the

1 http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm120709/debtext/120709-0001.htm#1207099000621

misuse of it. Focusing on the in principle, top level benefits of communications data without a consideration of these further issues can only lead to a one-sided debate.

16. The options presented in the Impact Assessment offer a further example of this issue, presenting a simple binary choice between 'doing nothing' and the Bill as written. This suggests either that there is only one way to address the capability gap, or that the Home Office has not considered alternatives.

17. The Privacy Impact Assessment does not offer much more detail, nor does it give a full consideration of the privacy issues. It is largely a description of some of the privacy risks and a statement that the safeguards are adequate, with no real analysis or explanation.

Lack of a public consultation

18. We regret that there has been no public consultation for this draft Bill. Whilst the Joint Committee have kindly called for written evidence, we are now significantly 'downstream' in the policy making process.

19. There was a consultation run by the previous Government on what is in its practical effects and implications the same proposal. Following this, and significant opposition to the ideas, the proposals were dropped before a draft Bill was published.

20. The current proposals may be argued to be substantially different from those developed by previous government, in which case they should be subject to a consultation. Or the proposals may be very similar, in which case there should be an explanation about why the Home Office has now drawn a different conclusion from the responses to the previous consultation. The Government appears to see this as a different proposal from the one put forward by the previous government. For example, Foreign Secretary Hague stated in Parliament:

> *"It differs enormously, because the previous Government's proposal was to hold all data in a central database. Our proposal would require providers to hold on to their data."*[2]

21. First, this is to downplay the functionality of a distributed database across services providers done to a design specified by GCHQ, which will in practice be no less insecure or intrusive than a centralised store. Second, as Privacy international and others have noted[3], the previous Government dropped proposals for a central database. Furthermore, Section 20 appears to allow for the creation of centralised services. So this is not a point of differentiation.

22. In the recent Demos report "#Intelligence", the authors (former director of GCHQ Sir David Omand, Jamie Bartlett and Carl Miller) make a similar point - that the regulation of the use of social media information (which they term 'SOCMINT') requires a more fundamental debate about what is appropriate:

> *The Government should publish a green paper as soon as possible on how it plans to manage over the next few years the opportunities offered by social media analysis and the moral and legal hazards that the generation and use of SOCMINT raises. This needs to include definition of the potential harms that SOCMINT pose, how harm can be judged and measured, and how these risks can be balanced and managed. It is important that the Government provides a position on the practicalities and specifics involved, including information on the relationship between the Government, ISPs and social network providers, the scope of information collected, the bodies authorised to collect it, who will have access to certain capabilities and with what safeguards.*[4]

23. The paper discusses the differences between private and public social media information. It can be seen as a broad argument that any changes in the types of data gathered and used for intelligence purposes must be accompanied by a wide public consultation, because of the different levels of intrusion that new types of communications data bring. In skipping to a draft Bill that focuses on the highly intrusive matter of communications data in such limited detail, albeit with the scrutiny of the Joint Committee, the government is short circuiting that broader public debate. We are also concerned that this places the Joint Committee in an extremely difficult position.

2 http://www.theyworkforyou.com/debate/?id=2012-06-20a.863.1
3 https://www.privacyinternational.org/blog/the-draft-communications-bill-is-a-wasted-opportunity
4 Page 69, http://demos.co.uk/files/_Intelligence_-_web.pdf?1335197327

24. We believe that ahead of a draft Bill, the Home Office should have produced a Green Paper to allow for a full public debate, about acceptable surveillance in the contemporary information society, through a more open democratic process.

Unanswered questions

25. A number of questions remain unanswered due to the lack of detail published about the draft Bill. For example:

- To what extent will any "black boxes" be used to collect information? Even though the law specifies only communications data, will the black boxes not be able to routinely gather content as well? If not, how will they work?

- How many services genuinely will not co-operate? Where are they located? The government may attempt to impose collection or access duties on companies located overseas. There are legal arrangements for such access, so the government should consider what sort of changes might resolve this issue. Furthermore, it is unclear to what extent such duties can be imposed by the UK or in what circumstances.

  This is a wider legal question than just those relating to communications data. Is there evidence that international legal agreements are not functioning? Has such an analysis been undertaken?

  Twitter is an example that does not seem to support the Home Office's case. Twitter already hands over data following an appropriate legal request, including to UK police[5]. 11 user information requests were issued between 1st January 2012 and 30th June 2012. Only 18% of these were complied with[6]. Rejections may arise from the requesting authority failing to identify a Twitter account, requests that are overly broad, or where users challenge requests after being notified. US court orders can be obtained by UK police, at which point the data is handed over. It would be useful to examine why the success rate for these requests is 18%.

  Google operates via a different model. They do not require court orders but largely comply with local standards, publishing a transparency report of their handling of request. The transparency report reveals they complied with 64% of requests for user data from the UK Government. Would the discretion that saw 36% of requests refused disappear under these proposals? The current model, which lacks a legal process in the handing over of user data, is not ideal. But we are concerned that the draft Bill proposes to replace this not with a court process but a model of self-certification by requesting law enforcement bodies with no meaningful judicial oversight.[7]

- Frequently, data is retained on devices as well as companies, and can also be accessed that way. To what extent would this address the capability shortfall?

- How will encrypted data be treated? Does the effectiveness of the proposals depend on breaking the encryption on which we routinely depend for online transactions, including banking and e-commerce? If so is that a net gain or a net loss to business confidence and to security in the UK?

Costs and benefits

26. Hardly any information on the costs or benefits has been published. We have been provided with ball park figures with no justification made public. In the Impact Assessment accompanying the Bill, the details of the costs and benefits are listed as 'optional'. The Home Office's Office for Security and Counter Terrorism has rejected our requests under the Freedom of Information Act for any useful level of data about the costs and benefits analysis. On 23rd July we asked them to supply us with the "summary of workings made to create that estimate, as used to create the figure used in the Impact Assessment, giving breakdowns for the

5 *Treaty between the Government of Bermuda and the Government of the United States of America relating to Mutual Legal Assistance in Criminal Matters* (http://www.official-documents.gov.uk/document/cm76/7613/7613.pdf)

6 https://support.twitter.com/articles/20170002#

7 See http://www.google.com/transparencyreport/userdatarequests/GB/?p=2011-12

savings categories mentioned above." In reply, the OSCT turned down the request. In their explanation of the public interest test, they set out the following justification:

> *"Sensitive operational benefits expected as a result of the draft Communications Data Bill would prevent the publication of the information requested. We consider that release of this information would aid individuals and/or groups seeking to plan or carry out an attack or commit a crime.*
>
> *The information withheld includes who we have worked with which would highlight operational capability issues. Disclosure of these details would limit the effectiveness of the law enforcement agencies to prevent and detect crime.*
>
> *The information which relates to UK capabilities is considered to pose an unacceptable risk to the ability of the UK to safeguard national security; the disclosure of this information could be used to avoid detection.*
>
> *We have determined that safeguarding national security interests and law enforcement is of paramount importance and that in all circumstances of the case it is our opinion that the public interest clearly favours the non-disclosure of information covered by section 31(1)(a)."*

27. We have requested an internal review of this decision. On June 21st, we asked the Home Office the following, again under the Freedom of Information Act for "the likely costs or estimates of costs for the programmes of collection and storage of communications data expected to be created under the Communications Data Bill, and analysis made by or for the Home Office of the available technologies to fulfil the new programmes of collection and storage of communications data under the same Bill". In reply, we were told that the request was being rejected on costs grounds. We are working to narrow the request.

28. We are particularly concerned that the withholding of information on the basis of national security is inhibiting a legitimate debate, by the public or Parliamentarians about the detail of this draft Bill. While this approach may be reasonable for certain specific details and issues, it is not appropriate for general obligations imposed on companies that involve data collection potentially affecting every citizen, innocent or not. It again makes understanding the proportionality of the proposal very difficult.

29. There are two key issues to consider when judging whether the current process is a sufficient mechanism for scrutinising the proposals. First, have the public been provided with enough information and detail to enable a proper public debate about the proposals? Second, is the Joint Committee being supplied with the required information by the Home Office and relevant bodies to make a proper and informed judgement?

30. Taken together, the answer to these questions determine whether the scrutiny process constitutes the requisite level of public deliberation about the use of the Bill's proposed powers and associated technologies.

31. The Joint Committee's findings are likely to be taken by the Government as a conclusive judgement on the acceptability of the proposals. It is one thing to withhold potentially sensitive information from the public. It is another to withhold it from the Committee set up to scrutinise the proposals in Parliament.

32. With reference in particular to the lack of a full consultation, the paucity of information concerning the details of the Bill and the rejection of Freedom of Information requests, we would argue that this has been an insufficient process of scrutiny and public debate.

Privacy and consent

33. It has been argued that people care less about privacy now, evidenced by the proliferation of social networks on which people share all manner of personal details. Building on this, some may argue either that the Government should be able to benefit from this information to the same extent that Tesco or Facebook can, or that people will not mind if the Government shares in the usefulness of this trove of data. In his evidence to the Joint Committee, for example, Professor Anthony Glees made a similar point:

> *"...there is a philosophical point here, where you have people putting all sorts of intimate details about themselves quite freely on to the internet. What is private and what is public no longer means what it meant when I was a student 40 years ago. One does have to have that debate."*[8]

34. It hardly needs pointing out that people now share more of their everyday life than ever before, both voluntarily and involuntarily. This interest in sharing often personal details is enabled by technologies that give people new ways to connect with each other, carry out everyday tasks and organise their lives. Much of this change in behaviour is driven by a combination of our social instincts, consumer habits and the business models of many digital businesses. In return for sharing more information about ourselves, we often get something in return – whether it is cheaper goods, apparently 'free' online services or more fulfilling social lives.

35. The fact that people have taken to sharing more about themselves does not mean that the government can feel empowered to appropriate that information. It does not imply an automatic right or need for that information. Nor does it suggest a fundamental shift in attitudes towards a more general reckless or relaxed attitude towards privacy – certainly not to the extent that it would permit institutions to assume rights to access or use information. The use of information is based on an individual's context specific consent. People often lack knowledge or clarity of how information will be used or the terms of an agreement, with research demonstrating that people often make 'imperfect' decisions that do not fit with a perception of perfectly rational privacy decisions.[9]

36. The general direction of data protection legislation has been to address such issues through emphasising minimisation of data collection and requiring consent to be as clear and informed as possible. The proposals in the draft Communications Data Bill are heading in the exact opposite direction.

37. Sometimes people will not be able to make individual direct decisions about use of personal information. Access to communications data by public bodies would be one example. In those situations, law enforcement bodies exercise their authority through the use of personal information. To the extent that this is an intrusion into the private sphere, the rules governing this use need to be created through democratic, public debate.

8 Uncorrected evidence, page 25 http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

9 See for example "Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right To Privacy", Directorate General for Internal Policies, Policy Development: Economic and scientific policy, 2011 http://www.europarl.europa.eu/committees/fr/studiesdownload.html?languageDocument=EN&file=65871 and Ian Brown, "Privacy Attitudes, Incentives and Behaviours", 2011 at: http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1866299_code892424.pdf?abstractid=1866299

The scope of information collection and access

38. The Home Office argues that the draft Bill is needed to maintain existing powers. This is not credible. The scope and nature of information collected make the proposals far more than a simple maintenance of existing capability.

39. The Home Office argue that they want to close the capability gap from 75% to 85% data availability. We argue that this must be placed in the context of the general orders-of-magnitude proliferation of data, personal and otherwise. In their report on 'big data' in 2011, McKinsey predicted a 40% growth in global data generated per year, arguing that “we are generating so much data today it is physically impossible to store it all”[10]. The Home Office impact assessment for the draft Bill assumes that the 'total volume of internet traffic increases by a factor of ten over the 10 year period.”

40. No doubt this poses challenges to law enforcement. But it is not accurate to say that the insights law enforcement may gain from available communications data has reduced, even if the percentage of the amount of data available has reduced. We question the notion of a capability gap couched in percentage terms, and see this as much a qualitative issue.

41. Data generated now is of a markedly different type to phone records and other traditional types of communications data. A record of a phone call tells an investigator who called whom, when, and where. Even this 'traditional' communications data is intrusive. The Article 29 Working Party of European data protection commissioners argued that the Data Retention Directive (Directive 2006/24/EC) involved “an inherently high risk level that requires appropriate technical and organisational security measures. This is due to the circumstance that availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users’ private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression.”[11]

42. The new kinds of 'communications data' the Bill is aimed at collecting can paint a more intimate picture of our lives. Details of social media communications reveals likely political opinions, lifestyle preferences, social circles, habits and patterns of behaviour. Although only the fact that a particular website was accessed, and not the specific page, is to be recorded, such information can still speak volumes. The fact that someone repeatedly contacted Narcotics Anonymous, or Gaydar, or a political website goes some way to indicate significant aspects of their identity or personality.

43. By combining email, telephone and web access data, and mobile phone location history, one can deduce a detailed picture of an individual’s movements, habits and thoughts to a greater degree than phone records alone could offer.

44. Additionally, the same "heuristic" techniques used to identify spam e-mail could potentially be applied to large-enough bodies of communications meta-data to identify common patterns. Heuristics for spam say, for example: "these 100 messages are spam. Is this new message like them statistically". Consider a similar scenario: "these 100 messages related to a given political party. Is this message like them statistically"?

45. The distinction between 'content' and 'communications data' does not, in practice, easily hold. This is partially because of the difficulty of separating out content from 'communications data.'[12], but also because the category 'communications data' does not adequately account for the variety of types of data, and the possible intrusiveness of it – which ranges from Oyster card user data to Facebook likes and comments, LinkedIn groups, Twitter Direct Messages and so on. Separating out content does not necessarily reduce the intrusiveness of data to the degree that blanket collection and weaker safeguards are acceptable or proportionate.

The move to general surveillance of the population

10 McKinsey Global Institute, Big data: The next frontier for innovation, competition, and productivity, 2011 available at http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation

11 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf page 1

12 For a discussion of this issue see “Briefing on the Interception Modernisation Programme”, LSE, 2009, http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

46. The government is giving itself extremely broad powers to order any communications provider to collect and disclose communications data. The government hasn't said how collection might work, even though the way the data is collected is critical.

47. The Committee has heard that this is most likely to involve collection duties on Communications Service Providers and 'black boxes' being installed on ISPs networks, which will harvest communications data that can then be access by relevant government bodies. This will involve organisations collecting information that they otherwise would not because it goes beyond their normal business needs. The proposals represent a fundamental shift to general, mass surveillance of the population.

48. The collection and storage of data is outsourced to the privacy sector, making CSPs the servants of the state rather then of their customers. It creates the liability for substantial payments by Government to service providers, introducing costs that may escalate and prove hard to control. This happens just at the time where elsewhere Government is making huge and to some extent successful efforts to bring HMG's out-of-control spending on IT and services back under control.

49. The result will be the creation of a distributed[13] database of a wide range of information about everybody's communication.

Filters and data mining

50. The clauses on "filtering" (clauses 14-16) appear from the drafting notes to relate to identifying data associated with an individual from a query across datasets or databases. However, the technical ability to search and identify people will go much further, and will be hard to regulate.

51. Filtering arrangements, described as a 'search engine'[14] for the collected communications data, would allow complex questions to be asked of the database relating to suspects' social networks.

52. Combined with large-scale data collection it could completely change the economics of mass surveillance. For instance, the data could identify a protester who posts to a radical politics site, and their location at any given time. Their favoured contacts, those likely to be politicised and their locations could be identified. The data could in effect be used to monitor political activity, or any activity deemed unusual or deviant, to a finely grained level.

53. At present, the police make sparing use of mobile phone location data because they get charged by the phone companies – typically several hundred pounds per subject. Once the data are all collected into connected databases, the per-use cost will approach zero. Investigative methods that are at present only used for serious crimes like rape and murder will be available to investigate minor issues too.

54. Given the nature of the communications data involved and the volume of data available, the scale of the likely collection and the provisions for filtering, we do not believe that it is creditable to claim this is simply a case of maintaining of existing powers to collect communications data. This is a significant extension of capability to create something qualitatively different.

Mission creep

55. We are concerned about the inevitability of 'mission creep', and the risk that this new cache of communications data will be used for an increasingly broad range of purposes. Home Office officials were pressed by the Committee about whether the data would be used to investigate speeding or dog fouling. They were reluctant to rule anything out. Dr Julian Huppert asked in the Joint Committee evidence session[15]:

> *"The Chief Constable of Derbyshire, Mr Creedon, who is the ACPO lead in the area, said last month that he would consider it perfectly appropriate if he saw somebody texting or using a mobile phone while driving to use the communications data for that."*

56. In reply, Charles Farr did not rule this use of the data out, saying: "I think you would have to demonstrate necessity and proportionality; let me put it like that."

---

13 Meaning simply 'it's not all in one place'

14 http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf page 35

15 See page 5 http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf

57. We do not believe that the primary check on the purposes for which communications data can be used should be the judgement of the law enforcement bodies themselves of what is 'proportionate and necessary'. The broad questions about the proportionality and necessity of the collection and use of this data for different purposes are better discussed in a forum that can make democratically legitimate judgements about the trade-offs between public interest, security and privacy. This is a job for Parliament.

58. We note the recommendation in the Demos report #Intelligence, which suggests that use of 'SOCMINT' – their broad term for information generated through social media – be limited:

> "As UK legislation at present limits the work of the intelligence agencies to national security, the detection and prevention of serious crime, and the economic wellbeing of the nation, we believe this narrower 'sufficient and sustainable cause' restriction should apply to their use of SOCMINT as well." [16]

59. The purposes for which the draft Bill suggests communications data can be used are far too broad and vague. This is another reason the draft Bill should be axed.

Wrongful access and the security of the data

60. In addition to overly broad access under the law, through mission creep for example, there is a risk of unlawful access through the insecurity of the data.

61. Sensitive private information has, in the past, fallen victim to 'blagging'. From obtaining NHS records[17] to accessing the Police National Computer[18], it is clear that no store of information is completely safe. Given enough time, private data can – and, likely, will – be accessed unlawfully by someone who is sufficiently determined or unscrupulous. It is worth reflecting on the fact that for some twenty years, "everyone knew" that journalists working for News International (and some other firms) were unlawfully obtaining information by bribing police officers, blagging information from official databases, and conducting unlawful interception.

62. We are concerned about the security of the data that will be captured and stored under these powers. The extent to which the security of the data can be maintained is an important factor in considerations of how proportionate and necessary these powers are. As such, we would expect an analysis of the likely security issues should be part of the public debate about the Bill.

63. However, we have not seen any such public-facing analysis. We are concerned that there has not been a full independent analysis of the technology involved and the security of the collection and storage of data.

64. Whenever data is stored by a company there will be a risk that it will be lost, stolen, or damaged. Normally, that risk of loss or theft is offset by the importance of the business purpose for which the company is retaining the data. The more valuable the data, the more likely it will be that individuals or groups will attempt to obtain it. Lawful points of access to information provide an attractive target for unlawful activity. In 2005, more than 100 mobile phones belonging to members of the Greek government were unlawfully tapped, through an exploitation of lawfully placed backdoors in the devices[19]. In 2009 it emerged that former US President Bill Clinton's personal emails – lawfully collected – were unlawfully accessed by an intelligence analyst[20].

Risks of misuse

65. The phone hacking scandal and the revelations from the Leveson Inquiry help to demonstrate that the ability to access personal information will be exploited for a variety of reasons. There are many ways that the data involved could be misused in a manner that would affect whistleblowers, journalists and their sources, legal privilege and activists.

---

16 http://demos.co.uk/files/_Intelligence_-_web.pdf?1335197327 page 43

17 Leveson Inquiry, Statement of Matt Driscoll, News of the World - 21st March 2012

18 Leveson Inquiry, Statement of Assistant Chief Constable Jerry Kirkby - 21st March 2012 pp.22-23.

19 http://www.guardian.co.uk/business/2006/feb/07/newmedia.media?INTCMP=ILCNETTXT3487

20 http://www.wired.com/threatlevel/2009/06/pinwale

66. For example, the Bill would facilitate relatively easy access to the contact histories of possible suspected leaks or sources that matched with those of a particular journalist. The Bill attempts to make searches easier, and automated. The searches could also extend to location histories.

67. A government wishing to know which of twelve civil servants had leaked evidence of serious wrongdoing to a journalist might ask each CSP for a list of everyone these thirteen people had communicated with last week, and when. The data would be taken to a central point (assumed to be NTAC at GCHQ) and studied, from which it might emerge that civil servant number 3 had called the mobile phone of Professor X at 7 on Tuesday evening, and Professor X had then made a Skype call to the journalist.

68. In short, the data matching and sorting provisions within the Bill would make anonymity extraordinarily difficult to maintain, whilst placing surveillance tools into the hands of an extremely large number of police, intelligence and other operatives who work under insufficient scrutiny.

69. In Annex B for a briefing from Public Concern at Work (PCaW) regarding these powers and the possible dangers for whistleblowers. This helps demonstrate that access to information can be used for the purposes of malicious or personal vendettas or certainly reactions that are not in the public interest. PCaW detail cases of whistleblowers and leaks that have involved an overzealous reaction from authorities including the case of HMRC tax lawyer Osita Mba[21], who had raised concerns about special deals between HMRC and those with large outstanding tax bills:

> *"In early part of June this year the Guardian reported that the Information Commissioner's Office (ICO) has launched an inquiry into the way HMRC investigators obtained the personal information of Mba and his wife.*
>
> *The ICO received documents that show in October 2011 HMRC managers sent personal information, including Claudia Mba's address and four phones' numbers to the Department's Criminal Investigations Unit."*

70. Trust in public institutions and those in them is important. Most public servants and officials and those involved in law enforcement are likely trustworthy. However, a desire to trust institutions does not mean ignoring the possible motivations, incentives and vulnerabilities of the people working in them.

21 http://www.guardian.co.uk/politics/2012/jun/07/information-commissioner-hmrc-whistleblower

Problems with safeguards governing access

71. The Impact Assessment asserts (page 5) that 'RIPA place strict rules on when, and by whom, access can be obtained to communications data retained and stored by industry", which is designed to prevent unauthorised access. However, RIPA does not place strict enough rules on access.

72. The Bill promises the same 'safeguards' as provided in RIPA. This means that (with the exception of local authorities, who must now seek judicial approval) organisations such as the police will continue to nominate an internal 'designated person' to authorise access to the collected data of millions of people.

73. For law enforcement purposes, access to the data will simply require designated senior officers at those bodies to believe that it's "necessary to obtain the data" and that it is "proportionate to what is sought to be achieved."

74. We are concerned that this effectively means that there will be no external, meaningful and direct oversight of access requests. We believe this will be ripe for abuse and exploitation[22]. The safeguards over access need to be tightened up rather than used as a model for access to a much broader store of information.

The Interception of Communications Commissioner

75. The oversight of such 'internal authorisation' is performed through the retrospective analysis of a sample of authorised requests. Each year the Interception of Communications Commissioner (IoCC) and his inspectors review a subset of the applications to ensure that policy is being applied correctly. We welcome the increasing amounts of information that the inspector has published year on year.

The 'error percentage'

76. However, we are concerned about the figures purportedly identifying the error rate of RIPA requests. The IoCC report states that the error percentage is 0.18% in 2011[23]. This looks to us to be incorrect, and the report lacks important basic details about when, where and how often errors happen. As a result the IoCC report does not facilitate a proper independent analysis of how the oversight and sign-off regime is working.[24]

77. In 2011, the IoCC identified 895 authorisation errors. On page 30, the report states that this is the number reported to the Commissioner's office. Page 32 clarifies that 99 of the 895 errors were 'identified by my inspectors during the inspections', rather than having been reported to them.

78. Seventy seven of those discovered errors appear to have been discovered in local authorities. Local authorities account for .5% of the total number of RIPA requests in 2011 (the total being 494,078 requests).

79. On page 30 of his report the Inspector states that the 'error percentage' is 0.18%. This appears to have been calculated by dividing the number of reported and discovered errors by the total number of RIPA requests.

80. However, the total number of inspections undertaken – the sample size - is not published. We do not know what percentage of the 494,078 requests the IoCC team inspected. That means that the reported error figure of 0.18% means very little, if anything.

81. The cited figure of 0.18% would only identify the error percentage rate for the total number of RIPA requests if the IoCC team inspected every single request or they are confident that there are zero further errors in the uninspected requests.

82. To determine the necessity and proportionality of powers to collect and access communications data, it is critical to have a clear picture of the error percentage. First, because it facilitates a proper understanding of the likely 'collateral intrusion'. Second, because it helps us to understand the likely frequency of false positives.

22 For more information on weaknesses in the current regime, we note the Big Brother Watch report 'A legacy of suspicion', available at http://www.bigbrotherwatch.org.uk//files/ripa/RIPA_Aug12_final.pdf

23 Page 30, IoCC report 2011

24 This issue was initially noted by Caspar Bowden

83. The error percentage has been used as evidence of how robust the current oversight regime is. For example, the figure from 2010 (0.3%) is cited on page 11 of the Home Office's Privacy Impact Assessment for the draft Bill. The IoCC himself states on page 30 of his report that he is 'satisfied that the overall error rate is still low when compared to the number of requests that were made during the course of the reporting year'.

84. Errors can have serious consequences. We know that two members of the public were wrongfully detained in 2011 as a result of RIPA related errors[25]. A certain number of mistakes are inevitable, but it is clear that the police occasionally use retained data to conduct invasive operations without sufficient verification.

85. In his evidence to the Joint Committee, Charles Farr makes the point that understanding the effectiveness of the authorisation regime is critical to examining how appropriate the powers are:

> *"the trivialisation of the use of communications data is therefore better tackled through an examination of the application process and the extent to which necessity and proportionality are, indeed, ingrained in the system. That feels, to me, a more likely route to avoiding trivialisation than defining or redefining serious crime, which, as you rightly say, is fraught with hazard. I personally believe that the necessity and proportionality tests are met by the users who use most of this data—the police—but you will come to a view on that."*[26]

86. It is crucial that the issue of sample size and error percentage is clarified. It is only possible to examine how appropriate such powers are when there is transparent oversight that inspires the full confidence of stakeholders.

87. We have written to the Commissioner to ask them to publish the sample size (ie the number of requests inspected), and to clarify the error percentage calculation. So far, their response has been to confirm that the number of requests inspected cannot be published. We have written a further open letter, which will be published on our website, highlighting the apparent calculation error and requesting an explanation. We will supply details of any reply to the Committee.

88. We recommend a review of the oversight of the access regime, for example looking at whether the IoCC has the required technical and legal staff, and the extent to which it relies on the police and agencies for advice. We also recommend an analysis of what information the IoCC should disclose to ensure full and transparent oversight of the access regime. This should be designed from the 'outside in', starting from the perspective of trying to ensure proper democratic oversight.

89. We recommend that, in addition to increased transparency of the workings of the oversight and inspection regime, those whose data is accessed are informed. This could be limited in cases where there are potential operational problems with informing the data subject.

90. As it stands, the safeguards are not transparent, and they do not command our confidence or the confidence of other knowledgeable observers. We are concerned therefore that the Home Office plans to step up to blanket data collection and retention with the same unsatisfactory oversight.

Incompatibility with human rights law

91. Annex A contains a legal opinion from Eric Metcalfe of Monckton Chambers regarding the compatibility of the draft Communications Data Bill. Metcalfe concludes that the Bill is incompatible with the UK's obligations under Article 8 ECHR on the basis that it fails to improve on the authorisation and oversight regime under RIPA and imposes a 'further requirement on CSPs and others to retain, make available and filter communications data for the purposes of lawful surveillance. In the absence of sufficient safeguards, this constitutes a further, disproportionate interference with the right to privacy".

92. Explaining the position on the insufficiency of the current safeguards, Metcalfe sets out that Article 8 requires access to communications data be governed by legislation the provides "adequate and effective safeguards against abuse" (para 15). He argues that the senior figure responsible for authorising access

25 http://www.guardian.co.uk/uk/2012/jul/13/snooping-errors-wrongful-detention-watchdog

26 http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf page 5

under RIPA 'cannot be credibly described as sufficiently independent or objective to provide an effective safeguard against arbitrariness or abuse" (para 16).

93. On the new powers to order collection and access to more communications data, Metcalfe argues that "the Bill's power to require CSPs to store, make available and filter their customers' private communications data in a particular manner for the sake of making covert surveillance easier" is "plainly disproportionate" (para 29).

94. The full opinion can be found at Annex A.

Retention is being challenged in many jurisdictions

95. The Data Retention Directive and its implementation are subject to legal challenges across Europe. In January of this year, Digital Rights Ireland asked the European Court of Justice to consider whether the Data Retention Directive is consistent with EU law[27]. The implementation of the Data Retention Directive is also being challenged in various forms in Germany[28], Bulgaria[29], Romania[30], Cyprus[31] and Czech Republic[32]. We consider it unwise to propose further collection and retention measures when the scope and implementation of the current Directive are being challenged across Europe.

96. The Article 29 Working Group published a report in 2010 on the implementation of the Data Retention Directive and were critical of the implementation of the Directive across Member States. They recommended that the categories of data retainable under the Directive be considered exhaustive, and that "the list of serious crimes justifying retention under the directive should be laid down at domestic level based on national law, taking into account the considerations...as for the need to clearly define and delineate what is meant by "serious crime.""

97. The Working Party were also very critical of the lack of statistics from Member States on the implementation of the Data Retention Directive, which meant a full review of the implementation of the directive was impossible. It seems unwise to propose an extension of the types and amount of information collected and stored whilst the impact of the current Directive is unclear.

27 See http://www.thejournal.ie/ecj-asked-to-rule-on-mandatory-retention-of-phone-and-internet-data-339434-Jan2012/ and for the document submitted to the Court, see http://www.scribd.com/doc/97936957/Digital-Rights-Ireland-data-retention-challenge-Preliminary-Reference-Questions

28 http://www.totaltele.com/view.aspx?ID=473999

29 http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

30 http://www.edri.org/edrigram/number10.1/romanian-senate-rejects-data-retention

31 http://www.pcadvisor.co.uk/news/mobile-phone/3362812/czechs-consider-reintroducing-eu-data-retention-rules/

32 http://jurist.org/paperchase/2011/03/czech-constitutional-court-overturns-parts-of-data-retention-law.php