Investigatory Powers Review

Written submissions (H-V)

Some material has been redacted at the request of the author. This is indicated by *** in the text. Some contributors sent their submissions to the ISC Privacy and Security Inquiry and Joint Committee on the Draft Communications Data Bill. These are marked accordingly.

Morton H. Halperin

Multilateral Standards for Electronic Surveillance for Intelligence Gathering

I. The Formation of the Multilateral Standards

A coalition of the willing of democratic states should agree to a set of standards for the collection, retrieval from large databases, retention, use and dissemination of information related to all persons other than government employees.

The standards and procedures should be made public and should be enacted as legally binding laws in each nation party to the agreement. Such laws shall spell out publicly what actions are authorized and shall provide oversight procedures, notice to persons surveilled and procedures for seeking redress.

II. The Scope of the Standards

This agreement shall apply only to surveillance of private citizens.

Some or all of the states party to this agreement may choose to reach agreements on a bilateral or multilateral basis on the standards for surveillance of government officials or for the prohibiting of such surveillance. These agreements need not be made public.

The agreement shall provide that the states party to the agreement shall not conduct electronic surveillance for law enforcement purposes (where the primary objective is to obtain evidence for criminal prosecution) on the territory of the other states party to the agreement or directed at the citizens of such states except on their own territory. Rather, states shall rely on existing mechanisms for cooperation on criminal investigations

The agreed-upon standards and procedures should be consistent with existing international law requirements, but may impose restrictions beyond those required by international law as a matter of policy and mutual agreement.

The development of the standards should start with the premise that there should be no difference in the standards for the surveillance of citizens of a country and the surveillance of the citizens of other countries covered by the agreement. Countries party to the agreement would thus seek to agree on common standards to apply to their own citizens and to others. Any deviation from common standards for citizens and others should be clearly identified and publically justified.

(The US President's Review Group recommended that the US should grant greater privacy protection to non-US persons than it does now, but less than that afforded to US persons. It recommended that such surveillance should be directed exclusively at the national security of the United States and its allies and should not be to obtain commercial gains for private industry. It suggested that the surveillance not be based exclusively on a person's political views or religious convictions. It proposed increased oversight and transparency. The panel justified providing greater protection to US persons because of the danger that the information collected might be used to affect the political process in the United States. The US Presidential Directive directed greater protection for non-US persons and for comparable treatment of personal information to the degree possible)

III. Activities Covered By the Standards

The standards should cover the following activities:

1. Targeted surveillance of a specific person where the interception of the communication is in the country conducting the surveillance, in the country of the person being surveilled, or in a third place.

2. The search of a data base under the control of the government for information about a specific named person whether the data is collected by "bulk collection" or other means. (This assumes that the agreed procedures will not prohibit bulk collection or other means to collect large data bases and that states will adopt legally binding and public rules specified when and how such collection may take place and justifying its legality)

3. The retention, use, or dissemination (within a government or to other governments) of personally identifiable information relating to a citizen or resident of a country covered by the agreement.

IV. The Contents of the Standards

a. The General Scope of Surveillance:

The targeted surveillance for intelligence purposes of a citizen or resident of any country which is party to the agreement, regardless of where the person is or where the interception is made, should be conducted under the same rules and procedures as the surveillance of citizens of the state conducting the surveillance.

These rules should require prior judicial authorization of the surveillance based on a probable cause standard that the target of the surveillance is engaged in illegal activity and that the primary purpose of the surveillance is not to gather evidence for a criminal prosecution but rather to gather intelligence to prevent a terrorist attack. The procedures shall require notice to the target when and if that would not defeat the purpose of the surveillance and shall provide for oversight by the legislature and the courts with the power to grant administrative and judicial redress.

(The United States under FISA permits surveillance of US persons, whether in the US or abroad, only with a warrant issued pursuant to the FISA standards. Other persons in the US can be surveilled based on a somewhat different standard with a FISC order. As with much of FISA, critical distinctions between standards for collection of US persons and others was spelled out in the definition section by providing for two definitions of "agent of a foreign power": one for "any person other than a United States person," and the other for "any person." In general non-US persons may be more easily subject to surveillance with less need to show a nexus to illegal activity; additional differences in the treatment of US persons and others appears in other definitions. For example, foreign intelligence information may be collected from a non-US person under FISA if it "relates" to the ability of the United States to protect itself from enumerated threats. However, if the target is a US person, the information must be "necessary" to protecting

the United States in order for it to be collected. Similarly, information about a foreign power relating to defense or foreign affairs may be collected from a non-US person, but may be collected from a US person only if "necessary." The difference in standards was written into FISA primarily to permit surveillance of Soviet nationals residing in the US ostensibly as private citizens. There has been no consideration since the end of the Cold War as to whether these distinctions need to be maintained.

Non-US persons outside the US can be surveilled if the interception occurs in the United States based on a court order under sect. 702 which permits surveillance of categories of targets. If the surveillance occurs outside the United States, it is subject to the much more permissible standards of the Executive Order on Surveillance (EO 12333) and requires no court supervision. The US Presidential Directive provides that information cannot be collected for the purpose of suppressing or burdening criticism or dissent or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation)

c. The Use of Government Databases:

The agreed-upon standards will need to specify whether governments are authorized to do "bulk collection" or to acquire large data bases by other means. There should be a heavy presumption against authorizing such collection. A proposal to include such authorization should be publicly defended and should carefully balance privacy and civil liberties concerns against the value of the collection. Any such authorization should be embodied in law and specify the scope of such surveillance.

If such data bases are authorized the agreement should provide that databases in the possession of governments party to the agreement can be searched for information about a specific private citizen only pursuant to specific guidelines and procedures and only if there is reasonable articulated suspicion that the target is one that could be subject to direct surveillance and that the information to be obtained relates to international terrorism. It should prohibit such searches to gather foreign intelligence in general. Oversight, notice and redress procedures should also apply to such searches.

(When FISA was enacted the focus was on the "wiretapping" of a specific phone. Minimization related to those who were overheard incidentally because they were talking to the target of the surveillance. Now much of the data collected by the NSA and other intelligence agencies is not limited to the transactions on a particular phone or computer. Until recently the USG took the position that as long as the data in its possession was lawfully acquired, there were no limits on how it could be used. Now the FISC has imposed limits on the ability of NSA to search the database acquired under sect. 214 and the US President in his Policy Directive has ordered limits on the searching of databases collected through "bulk collection," defined as acquiring a particular full stream of phone calls or emails without identifiers. The Directive provides that bulk collection data can be searched only for specified categories of information including terrorism, proliferation, and cyber threats, but not for foreign intelligence collection in general. The NSA does not consider the data acquired under sect. 702 to be "bulk collection" because the predicate is specified targets, even though it results in the collection of data far beyond a single phone number or email address.)

d. The Use of Personally Identifiable Information:

Finally, the agreed-upon guidelines and procedures should provide for limits on the retention, use, and dissemination of personally identifiable information of any private citizen of a country covered by the agreement. The agreement should provide that all such information should be destroyed unless it meets the standards for collection. The identification of a particular person should be deleted unless it is necessary to assess the value of the information. No information should be disseminated unless it is relevant to national security.

(The US Presidential Policy Directive on Signals Intelligence Activities provides that the term “personal information shall be applied in a consistent manner to US persons and non-US persons and that “to the maximum extent feasible consistent with national security” be applied equally to all persons regardless of nationality. The US intelligence community is now considering how to implement that directive.)

March 2014

Current and future threats

1. The UK faces a variety of threats to its national security. The UK government's National Security Strategy of 2010 outlines that these include, '[t]errorism, cyber attack, unconventional attacks using chemical, nuclear or biological weapons, as well as large scale accidents or natural hazards'.[1]

2. Of these, it faces a 'severe' threat from international terrorism, meaning an attack is 'highly likely'.[2] Charles Farr, the Director General of the Office for Security and Counter-terrorism has stated that Islamist terrorists pose the 'principal terrorist threat' to the UK;[3] and according to Andrew Parker, the Director General of MI-5, there have been 'serious attempts at major acts of terrorism in this country typically once or twice a year' since 2000.[4]

3. Technological advancements have made state attempts to counter this terrorist threat ever more challenging. In November 2013, Sir Iain Lobban, the Director of Government Communications Headquarters (GCHQ) commented that he believed technological changes had 'helped the terrorists', as the internet 'gives them a myriad of ways to communicate covertly. It gives them a platform, to fund-raise, to radicalise, to spread propaganda. It gives them the means to plan, to command and control, to spread lethal ideas, to exhort violence'.[5]

4. Similarly, Sir Malcolm Rifkind, the Chairman of the Intelligence and Security Committee of Parliament (ISC), has stated that, '[a]t the heart of the development of the international terror networks that most threaten our safety is the rise and spread of the internet…[terrorists are]

[1] 'A Strong Britain in an Age of Uncertainty: The National Security Strategy', HM Government, October 2010, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

[2] 'Protecting the UK Against Terrorism', HM Government, 12 December 2012 (last updated 3 September 2014), available at: www.gov.uk/government/policies/protecting-the-uk-against-terrorism.

[3] Witness Statement of Charles Farr to the Investigatory Powers Tribunal, 16 May 2014, available at: www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf.

[4] 'Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI), Whitehall', 8 October 2013, available at: www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-at-rusi-2013.html. See also: Simcox, R.; Stuart, H.; and, Ahmed, H., Islamist Terrorism: The British Connections, *The Henry Jackson Society*, 2011 (Second Edition).

[5] 'Uncorrected Transcript of Evidence', Intelligence and Security Committee of Parliament, 7 November 2013, available at: www.globalsecurity.org/intell/library/reports/2013/20131107_isc_uncorrected_transcript.pdf.

communicating online, using e-mail, social messaging, peer-to-peer sharing sites, chat rooms, webcams, online gaming platforms, mobile applications and a whole host of other media'.[6]

5. It is not just those tasked with protecting national security that have highlighted the difficulties these changes have caused. As Mark Hughes, speaking as Head of Corporate Security at Vodafone, outlined: '[n]o longer are customers just making telephone calls and sending text messages. All our organisations connect customers to the internet, and then they can choose from a range of third-party applications to have those conversations'. Hughes believes that this would cause 'significant disruption' to law enforcement and security investigations'.[7]

6. Therefore, the UK faces a plurality of threats, and changes in technology have impacted the state's ability to safeguard against these threats.

Communications data

7. There are three specific types of communications data of particular relevance to the government.

   (a) **Subscriber data**. This enables the state to find out, for example, information 'such as "who is the subscriber of phone number 012 345 6789?", "who is the account holder of e-mail account xyz@xyz.anyisp.co.uk?" or "who is entitled to post to web space www.xyz.anyisp.co.uk?"';[8]

   (b) **Use data**. This enables the state to find out, for example, information such as 'itemised telephone call records (numbers called); itemised records of connections to internet services; itemised timing and duration of service usage (calls and/or connections)';[9]

   (c) **Traffic data**. This enables the state to find out, for example, information such as 'tracing the origin or destination of a communication that is in transmission [and] the location of equipment when a communication is or has been made or received (such as the location of a mobile phone)'.[10]

8. According to Home Secretary Theresa May, communications data 'is about the who, when, where, and how'.[11]

9. Communications data is a vital tool in safeguarding national security. The Home Secretary has stated that it 'has played a significant role in every Security Service counter-terrorism

[6] 'Wadham Lecture: "Intelligence Agencies in the Internet Age – Public Servants or Public Threat", Sir Malcolm Rifkind MP, Chairman of the Intelligence and Security Committee of Parliament', 8 May 2014, available at: www.wadham.ox.ac.uk/docs/WadhamLecture852014_1399967593.pdf.

[7] 'Oral Evidence; Draft Communications Data Bill; Joint Committee on the Draft Communications Data Bill, House of Lords & House of Commons' 2012-1013, available at: www.parliament.uk/documents/joint-committees/communications- data/Oral-Evidence-Volume.pdf.

[8] Draft Communications Data Bill, HM Government, June 2012, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf.

[9] Ibid.

[10] Ibid.

[11] Report, together with appendices and formal minutes: Draft Communications Data Bill; Joint Committee on the Draft Communications Data Bill, House of Lords & House of Commons' 2012-1013, available at: www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf.

operation over the last decade. It has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service'.[12]

10. Similarly, a Parliamentary Joint Committee on the Draft Communications Data Bill has stated that, 'communications data is an invaluable weapon in the defence of national security and in the fight against crime—especially terrorism and other serious crimes'.[13]

11. The 'other serious crimes' outside of mass casualty terrorism that data communications helps prevent can sometimes be overlooked in public discourse. Yet data communications are absolutely fundamental to preventing child abuse and exploitation (or prosecuting its perpetrators); identifying and locating those at risk of suicide; identifying rapists or kidnappers; reconstructing organised crime networks; and murder investigations.[14]

12. However, there is concern within government that the ability of the state to protect the public from serious crime is diminishing due to degradation in the government's ability to use communications data.[15] The government has stated that is has a 25% data gap, in that 'public authorities can no longer get access to the data that they would want',[16] although the accuracy of this figure has been called into question by the Parliamentary Joint Committee on the Draft Communications Data Bill.[17]

13. In April 2012, it emerged that the Home Secretary intended to introduce new legislation which seeking to address the state's supposed diminishing ability to access communications data. This proposal faced significant opposition from the Liberal Democrats, including from Deputy Prime Minister Nick Clegg,[18] as it was interpreted as overly intrusive from a civil liberties point of view.

14. The legislation was scrutinised by the Parliamentary Joint Committee on the Draft Communications Data Bill, which concluded that the bill paid 'insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data'.[19]

15. Agreement was unable to be reached within government about how to proceed and the issue of ensuring continued access to required communications data has remained unaddressed.[20]

---

[12] Communications data and interception, HM Government, 10 July 2014, available at: www.gov.uk/government/speeches/communications-data-and-interception.

[13] Report, together with appendices and formal minutes: Draft Communications Data Bill; Joint Committee on the Draft Communications Data Bill, House of Lords & House of Commons' 2012-1013.

[14] Uncorrected Transcript of Oral Evidence: Data Communications Data Bill, House of Lords & House of Commons, 12 July 2012, available at: www.parliament.uk/documents/joint-committees/communications-data/uc120712Ev3HC479iii.pdf.

[15] Oral Evidence; Draft Communications Data Bill; Joint Committee on the Draft Communications Data Bill, House of Lords & House of Commons' 2012-1013.

[16] Ibid.

[17] 3; Is there a need to access more communications data?; Draft Communications Data Bill; Draft Communications Data Bill Joint Committee, HM Government, available at: www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7906.htm#a9.

[18] 'Nick Clegg pledges open hearings over web surveillance plans', *The Guardian*, 3 April 2012, available at: www.theguardian.com/politics/2012/apr/03/nick-clegg-open-hearings-surveillance; see also: 'Nick Clegg tries to head off Lib Dem revolt over email surveillance plans', *The Guardian*, 3 April 2012, available at: www.theguardian.com/uk/2012/apr/03/theresa-may-email-surveillance-plans.

[19] Summary; Draft Communications Data Bill; Draft Communications Data Bill Joint Committee, HM Government, available at: www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7903.htm.

[20] 'Clegg speech: We saved UK from "snooper's charter," ID cards and tax breaks for the rich… Lib Dem leader launches bid for 2015 election', *The Independent*, 18 September 2013, available at: www.independent.co.uk/news/uk/politics/clegg- speech-we-saved-uk-from-snoopers-charter-id-cards-and-tax-breaks-for-the-rich-lib-dem-leader-launches-bid-for-2015- election-8824451.html; 'Blow to Theresa May as Clegg vetoes her "snooper's charter"', *The Times*, 25 April 2013, available at: www.thetimes.co.uk/tto/news/politics/article3748477.ece.

16. A 2013 poll showed the general public were largely sympathetic to proposed changes in the law giving the government greater access to communications data.[21] Furthermore, despite the media's disclosures of the classified documents stolen by former NSA contractor, Edward Snowden last year, this did not lead to public clamouring for reining in state's powers. In the UK, more people regarded the leaks as a 'bad thing' than a 'good thing'.[22]

17. Therefore, there appears to be public sympathy for the notion that safeguard national security is a challenging task and the police and Security Services require relatively broad powers in order to do so.

Regulation of Investigatory Powers Act (RIPA) 2000

18. RIPA is a core piece of legislation which assists law enforcement and intelligence agencies in protecting national security and solving serious crimes.

19. RIPA 'provides the statutory framework which governs the interception of communications'.[23] It allows the government 'to regulate who could access communications data, what classes of data they could access, for what purposes, and subject to what controls' but 'does not regulate what data must be retained, dealing only with acquisition and disclosure'.[24]

20. According to Charles Farr, '[i]nterception under RIPA provides tactical information [and] real time intelligence on the plans and actions of individual terrorists, criminals and other targets […] and facilitates their arrest by law enforcement agencies'.[25] This intelligence has 'led directly to the prevention of terrorist attacks and serious crime, the success of operations aimed at countering the proliferation of weapons of mass destruction and the saving of lives'.[26]

21. However, the pace of technological change has led to debate as to whether RIPA is fit for purpose in meeting these advancements and how it should handle the new types of data being generated (for example, from social media). There is concern as to the correct balance in terms of the state's ability to encroach on individual privacy, and whether it is being used correctly and proportionately.

22. The idea that RIPA would eventually need updating was even being discussed when the legislation was initially passed. For example, during a House of Commons debate in March 2000 concerning RIPA, Mike Gapes MP commented that 'I, like hon. Members on both sides, am concerned that it may well become out of date very quickly…we must recognise that we

[21] 'YouGov / Huffington Post Survey Results', *YouGov*, 2013, available at: cdn.yougov.com/cumulus_uploads/document/ht3d0v7dg6/Huffington-Post-results-130610-Snoop.pdf.
[22] Dahlgreen, W., 'Little Appetite for Scaling Back Surveillance', *YouGov*, 13 October 2013, available at: yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/.
[23] Regulation of Investigatory Powers Act 2000: Proposed Amendments Affecting Lawful Interception – A Consultation, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/157983/ripa-lawful-intercept-responses.pdf.
[24] History and Background; Draft Communications Data Bill; Draft Communications Data Bill Joint Committee, HM Government, available at: www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7904.htm.
[25] Witness Statement of Charles Farr to the Investigatory Powers Tribunal, 16 May 2014.
[26] Ibid.

may have to revisit this subject in two, three, five or 10 years' time, depending on how fast and how far these matters advance'.[27]

23. There are now increased calls for reform.[28] That RIPA may need to be amended has been posited by senior political figures such as the former independent reviewer of terrorism legislation Lord Carlile and Shadow Home Secretary Yvette Cooper.[29]

24. Reforming RIPA, however, is a high-risk strategy that would likely lead to demands for changing sections of the legislation which are fundamental to GCHQ's work but controversial among particular media outlets and NGOs.

25. One example of this is Section 8(4) of RIPA. Interception under Section 8(4) takes place via state tapping of fibre-optic communication cables carrying both external (i.e. communications sent or received outside the UK) and internal communications (i.e. communications sent and received inside the UK).

26. As even internal communications may be transited via internet service providers in foreign nations, it is impossible to separate, or filter out, what are internal and what are external communications when the state initially scoops this data up.

27. RIPA gives GCHQ relatively broad powers to intercept external communications using a general warrant that does not require a specific named subject to be on it. The interception of internal communications without a named warrant has provoked controversy – as has the volume of overall communications captured.

28. However, there is a practical reason for its use. According to Farr:

> Within the British Islands, the government has sufficient control and considerable resources to investigate individuals and organisations, and it is feasible to adopt an interception regime that requires either a particular person, or a set of premises, to be identified before interception can take place. Outside the British Islands, the government does not have the same ability.[30]

This is because the government is often unaware of, for example, the precise geographic location of al-Qaeda operatives abroad or cyber criminals, and is unlikely to have 'the same practical ability to identify the apparatus over which these communications were to be carried; nor the same practical power to obtain messages'.[31]

29. Farr has stated that, in these circumstances, 'the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it

---

[27] Parliament home page; Parliamentary business; Publications and Records; Hansard; Commons Debates; Commons Debates by date; Commons Debates - previous sessions; Bound Volume Hansard – Debate, available at: www.publications.parliament.uk/pa/cm199900/cmhansrd/vo000306/debtext/00306-11.htm.

[28] Moore, M., 'RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework', *The Political Quarterly*, Vol. 85, No. 2, April-June 2014, available at: www.academia.edu/7895161/RIP_RIPA_Snowden_Surveillance_and_the_Inadequacies_of_our_Existing_Legal_Framework.

[29] Parliament home page; Parliamentary business; Publications and Records; Hansard; Commons Debates; Daily Hansard - Westminster Hall, 31 October 2013, available at: www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm; see also: 'The challenges of a Digital World to our Security and Liberty – Yvette Cooper speech to Demos', Labour Press, available at: press.labour.org.uk/post/78448368189/the-challenges-of-a-digital-world-to-our-security-and.

[30] Witness Statement of Charles Farr to the Investigatory Powers Tribunal, 16 May 2014.

[31] Ibid.

is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of these communications for examination...'[32] This can be vital in discovering overseas terrorist attack planning, for example.

30. Furthermore, internal communications can only be looked at, listened to or read (under provisions in Section 16 of RIPA) in limited circumstances. The Secretary of State must certify that its examination is necessary for a national security or serious crime purpose; or if the individual whose communications were being examined under a Section 8(4) warrant was thought to be abroad but it has just been discovered is actually in the UK.[33]

31. The Interception of Communications Commissioner – whose responsibility is 'to keep under review the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities'[34] – recently concluded that this process did not have 'any significant risk of undue invasion of privacy'.[35]

32. The Section 8(4) issue is particularly pertinent with regards to social media. Popular social media platforms such as Facebook and Twitter (collectively used by over 1.5 billion people)[36] did not even exist when RIPA was passed, and there is concern that the state is interpreting RIPA's powers too broadly and subsequently being overly intrusive on this front.

33. The storage and ability to access this type of data has proven controversial among privacy groups and sections of the media and led to increased calls for RIPA reform.[37]

34. At present, Google and YouTube searches, Twitter 'tweets' and Facebook 'posts' are generally defined by the state as 'external communications'. This is not only because Google's data centres and Twitter, YouTube and Facebook's web servers are based outside the UK (usually in the US); but also because as there is not a known recipient of the search or the post, it cannot shown to be an internal communication.[38]

35. The situation with emails is different (including personal email messages sent via social media platforms such as Facebook). As long as the sender and recipient are based in the UK, this will be defined as an internal communication, even though the servers used by webmail services (such as Hotmail) are not based here.

36. Some have argued that the state's ability to access of social media intelligence should be put on a stronger 'legal footing'.[39] The importance of communications data in tackling terrorism and serious crime means that provisions around the state's ability to legally intercept communications data needs to be on as firm a legal basis as possible.

---

[32] Ibid.

[33] May, A., '2013 Annual Report of the Inception of Communications Commissioner', Interception of Communications Commissioner's Office (IOCCO), 2014, available at: www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

[34] 'Home', Interception of Communications Commissioner's Office (IOCCO), available at: www.iocco-uk.info/.

[35] May, A., '2013 Annual Report of the Inception of Communications Commissioner', Interception of Communications Commissioner's Office (IOCCO), 2014.

[36] 'Our Mission', *Newsroom*, available at: newsroom.fb.com/company-info/; 'About', *Twitter*, available at: about.twitter.com/company.

[37] 'Social media mass surveillance is permitted by law, says top UK official', *The Guardian*, 17 June 2014, available at: www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr.

[38] Witness Statement of Charles Farr to the Investigatory Powers Tribunal, 16 May 2014.

[39] Omand, D.; Bartlett, J.; and, Miller, C., 'A balance between security and privacy online must be struck', *Demos*, 2012, available at: www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327.

37. Another area in which RIPA is potentially outdated is regarding the distinction between communications data and content.

38. This splitting of communications data and content into two parts allows authorities to better balance the intrusiveness of their investigation. As it has traditionally been less intrusive to look at communications data than actual content, the level of authorisation and proof for the interception is lower.

39. However, technological advancements now allow large amounts of personal information to be gleamed from communications data under the less stringent procedures.

40. With access to communications data, investigators are able to piece together a comprehensive picture of people's lives from a variety of communications data sources revealing and monitoring their movements, habits, social networks and interests. As the Information Commissioner has noted, 'communication records… can be highly intrusive even if no content is collected.'[40] As a result, the boundaries between content and communications data have become increasingly blurred.[41]

41. Some have interpreted this as a growing encroachment on privacy, arguing that the volume of information, level of detail, and the possible implementation of what is revealed by communications data is now in many ways equal to that of content.[42]

42. Even if RIPA is amended because of such issues, it must remain technologically neutral. Referencing specific technology and communication methods would mean the legislation not only becomes quickly outdated and invites constant revision, it could overly restrict the state's ability to gather certain types of intelligence.

43. Any reform of RIPA – even tweaks of the legislation – must ensure that the state's capacity to access the data needed to keep the country safe is retained.

The effectiveness of current statutory oversight arrangements

44. Stringent oversight arrangements are a necessity in order to gain public trust and consent for the activities of the state's intelligence agencies.

45. Statutory oversight pertaining to data communications and interception comes from three separate sources: the ISC; various independent Commissioners (who report to the Prime Minister and provide a limited form of judicial oversight); and the relevant Secretaries of State, who are accountable to Parliament. Unlike comparable Western democracies, judicial authorisation is not required in the UK before interception warrants are issued (with the exception of local authorities who, from November 2012, were required to seek judicial approval).[43]

---

[40] 'Every phone call, email or website visit "to be monitored"', *The Telegraph*, 24 April 2009, available at: www.telegraph.co.uk/news/uknews/5215413/Every-phone-call-email-or-website-visit-to-be-monitored.html?mobile=basic. [41] 'The Snowden Leaks: The Need to Update our Legislation on Data and Security', *RUSI*, 31 October 2013, available at: www.rusi.org/analysis/commentary/ref:C527248CF8F8ED/#.VCVvPvldUus.
[42] 'Written Evidence to the Joint Committee on the Draft Communications Data Bill', JUSTICE, August 2012, available at: www.justice.org.uk/data/files/resources/330/JUSTICE-Draft-Comms-Data-Bill-FINAL-Submission-August-2012.pdf.
[43] 'Surveillance and counter-terrorism', HM Government, 26 March 2013, available at: https://www.gov.uk/surveillance-and-counter-terrorism

46. The ISC was created by the Intelligence Services Act 1994. It is the all-party parliamentary oversight body relating to GCHQ, the Security Service and the Secret Intelligence Service,[44] and the principal way in which the agencies can be scrutinised by Parliament.

47. Initially, the ISC existed largely to examine expenditure and other administrative functions of the Agencies' running. While it did have access to sensitive material, it only had what the current Chair of the ISC described as 'seriously restricted' powers to act as an effective oversight body.[45]

48. The Justice and Security Act 2013 (JSA) enhanced the scope of the ISC's investigatory powers in order to increase their ability to hold the intelligence agencies to account.[46]

49. There is little appetite within the ISC for further powers, as they do not think more are presently needed.[47] This is in part due to that face that, recent changes to the ISC's functions include the following:

    (a) the Chair is now appointed by the Committee, as opposed to the Prime Minister;

    (b) if the ISC requests information from the intelligence services, they now have a legal requirement to supply it. The ISC staff can even go into the office of intelligence agencies and, with agency staff, pick the files they wish to see.[48] Beforehand, the ISC could only 'request' such information. Only a Secretary of State can now withhold the information, as opposed to a head of one of the intelligence services.

    (c) a doubling in budget and rise in staffing;

    (d) formal responsibility given for oversight of Agency operations; the Security Service, the Secret Intelligence Service and GCHQ now have to provide detailed information on their operations on a quarterly basis.[49]

50. Two independent Commissioners also have oversight over GCHQ: the Intelligence Services Commissioner and the Interception of Communications Commissioner.[50] The latter overseeis all agencies that are able to apply for interception warrants (including GCHQ).[51]

51. Commissioners are independent from the government and the agencies of which they have oversight. They have no significant impact on policy, nor are they intended to. While they can make recommendations, according to Sir Malcolm Rifkind MP, commissioners act as the equivalent of 'accountants looking at a tax return. They don't look to see if tax policy is right or wrong'.[52]

52. There may be scope to review the role played by the Commissioners in any reform of RIPA, which could include:

---

[44] The Law; Oversight; GCHQ, available at: www.gchq.gov.uk/how_we_work/running_the_business/oversight/Pages/the-law.aspx.

[45] 'Wadham Lecture: "Intelligence Agencies in the Internet Age – Public Servants or Public Threat", Sir Malcolm Rifkind MP, Chairman of the Intelligence and Security Committee of Parliament', 8 May 2014.

[46] 'Intelligence and Security Committee of Parliament; Annual Report', 2012-2013, HM Government, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/211553/31176_HC_547_ISC.PDF.

[47] Author interviews with Sir Malcolm Rifkind MP and Hazel Blears MP, August – September 2014.

[48] 'Wadham Lecture: "Intelligence Agencies in the Internet Age – Public Servants or Public Threat", Sir Malcolm Rifkind MP, Chairman of the Intelligence and Security Committee of Parliament', 8 May 2014.

[49] Ibid.

[50] The Law; Oversight; GCHQ.

[51] Witness Statement of Charles Farr to the Investigatory Powers Tribunal, 16 May 2014.

[52] Author interview with Sir Malcolm Rifkind MP, August 2014.

(a) the extent to which the Commissioners' various tasks overlap;

(b) whether some of the Commissioners' functions could be amalgamated (as posited by Joint Committee on the Draft Communications Data Bill); [53]

(c) whether formerly serving as a high court judge must be a requirement for the role, or whether the scope can be widened to other individuals of high legal standing (as is the case with the independent reviewer of terrorism legislation position, for example);

(d) whether the commissioners need to take a more public role in explaining their work and clarifying misconceptions about the state's intercept abilities.

53. A further safeguard pertaining to RIPA is provided by the Home Secretary or Foreign Secretary, who must personally issue an interception warrant.

54. The Interception of Communications Commissioner has stated that 'The Secretaries of State themselves are entirely conscientious in undertaking their RIPA 2000 Part I Chapter I duties. They do not rubber stamp applications. On the contrary, they sometimes reject applications or require more information'.[54]

55. Despite the salacious headlines generated by Edward Snowden in 2013, those tasked with oversight of the Agencies have at no stage concluded that the state has acted in any way illegally.

56. In July 2013, the ISC issued a statement in response to allegations that GCHQ was illegally accessing communications data via PRISM, the US Government's data-mining computer system which enables the potential capture of content from foreign citizens' electronic communications. The ISC concluded that GCHQ did not break the law in regards to their interception of communications and conformed to its statutory duties.[55]

57. The Interception of Communications Commissioner stated in his most recent report that he had 'unrestricted access to full information, however sensitive' to carry out his review (all those agencies that RIPA applies to have a statutory obligation to provide such information).[56] He concluded not only do 'the Secretaries of State and the agencies that undertake interception operations under RIPA 2000 Chapter I Part I do so lawfully, conscientiously, effectively and in the national interest', but that RIPA was still fit for purpose.[57]

58. These are not conclusions that those suspicious of state overreach will share, but ones that should be considered when considering reform of RIPA and altering the state's interception capabilities.

Conclusion

59. There has been significant debate in the West regarding the correct balance between the sometimes competing concerns of liberty and security. This is understandable. While the

[53] Report, together with appendices and formal minutes: Draft Communications Data Bill; Joint Committee on the Draft Communications Data Bill, House of Lords & House of Commons' 2012-1013.
[54] May, A., '2013 Annual Report of the Inception of Communications Commissioner', Interception of Communications Commissioner's Office (IOCCO), 2014.
[55] 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', Intelligence and Security Committee of Parliament, 17 July 2013, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf.
[56] May, A., '2013 Annual Report of the Inception of Communications Commissioner', Interception of Communications Commissioner's Office (IOCCO), 2014.
[57] Ibid.

public cannot be given every operational detail, there must be broad public consent for the type of activities that intelligence and security agencies undertake.

60. The answer to these debates, however, may not necessarily be more state openness and transparency. As a society, we must also accept that sometimes there is a good reason for a lack of transparency and that more state disclosures and public knowledge is not always an unalloyed good.

61. There is a significant level of secrecy over the government's capacity to gather intelligence for a good reason. The alternative provides terrorists and other criminals with enhanced knowledge on how to avoid detection and significantly weakens our security and crime- fighting apparatuses. Without a strong national security policy that can protect citizens from mass-casualty terrorism and other forms of attack, retaining liberty, security and public order becomes impossible.

62. As citizens are increasingly choosing to share vast amounts of their private details online with corporations, the meaning of privacy is increasingly ambiguous.

63. Furthermore, the state has never had such an extensive technological capacity to be able to breach the civil liberties of its citizens. Yet that does not mean that it is doing so. In most regards, the UK's system is working correctly and it is tweaks, rather than major revisions, that are required.

Robin Simcox
Research Fellow at the Henry Jackson Society
October 2014

Human Rights Watch

Human Rights Watch respectfully submits the following information to David Anderson QC for the Investigatory Powers Review. Firstly, we explain the need to reform UK legislation governing surveillance to bring it in line with the UK's human rights obligations, in particular its obligations to respect and protect the right to privacy. Secondly, oversight of government surveillance by the Interception of Communications Commissioner is not comprehensive and it lacks the independence and transparency that are necessary for such a task. The government should address these shortcomings and create an authority that provides effective oversight of its surveillance activities.

Revelations by former National Security Agency (NSA) contractor Edward Snowden published by the *Guardian* included credible evidence that the Government Communications Headquarters (GCHQ) is engaged in the interception and collection of internet and phone data on a mass scale, in breach of the rights of millions of people in the UK and in other countries to privacy and to freedom of expression. Yet the UK government has failed to answer legitimate questions about its involvement in mass surveillance, asserting that the intelligence agencies complied with the law and acted to protect public safety.

While we fully accept that the UK government has a duty to protect national security and prevent crime, there is an important distinction between taking steps that are necessary and proportionate to achieve those aims and monitoring indiscriminately the communications of millions of people in the UK and other countries who are under no suspicion whatsoever. The UK's human rights obligations impose limits on the scope and scale of surveillance that the government may justify under the banner of national security.

The UK government should explain to the public the scope and magnitude of the alleged surveillance by the GCHQ as well as the authority and limitations under which it is conducted. The government should also clarify how much data on people located outside British territory is being gathered and how it is being stored, used, or shared with third parties, particularly since the legal protections against such interception are weaker for people abroad under UK law.

Reforming UK surveillance legislation in accordance with the right to privacy

Human Rights Watch holds that legislation in force in the UK is inadequate to protect against wholesale breaches of privacy rights and that any new legislation should ensure that communications data is intercepted only in exceptional circumstances. Any decision authorizing such interception should be subjected to independent scrutiny by a judicial authority.

Analysis of UK laws governing surveillance by Human Rights Watch has led us to conclude that the legislative framework in the UK does not adequately protect the right to privacy and allows for far-reaching government surveillance without effective independent oversight.

In July 2014, the UN Office of the High Commissioner for Human Rights (OHCHR) published a report that is highly critical of mass surveillance and calls on states to review their laws and bring them into line with international human rights standards. The report elaborated on state obligations to respect and ensure privacy when conducting digital surveillance. The report found that practices in many states have revealed "a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight." Combined with a "disturbing lack of governmental transparency," these failings have "contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy" (paras 47-48).

Under the European Convention on Human Rights (ECHR), and the Human Rights Act (HRA) which incorporates it into domestic law, the UK must respect the right to private life and any interference with this right must be "in accordance with the law" and "necessary in a democratic society," that is, no greater than needed to protect a legitimate state interest. As the OHCHR report states, the International Covenant on Civil and Political Rights (ICCPR), ratified by the UK, also prohibits arbitrary and unlawful interference with privacy, which requires surveillance measures to be not only according to law but also necessary and proportionate. This right applies to digital and phone communications and is not limited to the contents of those communications. The OHCHR has called on all states to "review their own national laws, policies and practices to ensure full conformity with international human rights law."

The UK government should bring up to date the law under which GCHQ has been acting, namely the Regulation of Investigatory Powers Act 2000 (RIPA), and bring it in line with advancements in technology and digital communication and the UK's international human rights obligations. In the years since the UK's new law on intercepting communications was introduced, digital surveillance capabilities have evolved dramatically and the government now has the duty to reform the legal framework to ensure it protects the right to privacy, given how technologies have evolved.

RIPA allows a senior government minister—a "secretary of state"—to issue a warrant at the request of a senior intelligence or police official. The warrant authorizes the interception of communications for which the sender or intended recipient is in the United Kingdom, if the secretary of state believes intercepting the information is necessary and proportionate.

In addition to permitting a warrant if it is "necessary" "in the interests of national security," the law permits a warrant if it is "necessary" for "preventing or detecting serious crime." The grounds for granting a warrant under the law remain very broad, even though the

recent Data Retention and Investigatory Powers Act (DRIPA) 2014 limited an additional reason of "safeguarding the economic well-being of the United Kingdom" to cases relating to national security.

RIPA distinguishes between communications between people located in the UK ("internal"), and those where the sender or recipient is abroad. For the latter, considered to be "external," the warrant does not need to specify a particular person or premises that may be linked to wrongdoing or actual security threats, creating a lower standard of protection for those communications. This lower standard for the interception of external communications enables extremely broad collection of personal data and communications of individuals who are not linked to any wrongdoing, thus breaching the principle of proportionality as well as those individuals' right to privacy.

As made clear by the government's written statement in the case brought by Privacy International, Amnesty International and other rights groups before the Investigatory Powers Tribunal on GCHQ's surveillance activities, the UK government treats searches on Google and YouTube, posts on Facebook, and tweets as "external communications" since the companies' web servers are largely based outside the British Islands, which means that the online communications of people in the UK may be intercepted with only the weak safeguards RIPA requires for "external communications."

This shows the inherent weakness of the RIPA regime, as well as the urgent need to update current legal frameworks for the digital realm. RIPA was enacted in 2000, before the advent of nearly all global social media services. Today, over a decade later, when individuals use social media or web-based email services, their data is routinely held in various jurisdictions around the world and can travel across multiple borders in seconds.

These concerns were not addressed by DRIPA, passed as emergency legislation in July, after the government gave parliament only three days to review it. On the contrary, the new Act extends the scope of those who may be subject to interception warrants to companies outside the UK that offer communications services to UK customers and extends the definition of "telecommunications service" to include "companies who provide internet-based services, such as webmail." This change subjects a much broader range of internet companies in the UK and abroad to surveillance warrants from the UK.

The government should safeguard the privacy rights of individuals whose communications it intercepts in the same way whether they are inside or outside the UK. Indeed when a country can exercise control or jurisdiction over the digital communications of non-citizens, or people outside its borders, in a comprehensive or wholesale fashion, it also assumes an obligation to respect those people's rights. This principle was most recently affirmed by the OHCHR's report on the right to privacy in the digital age, which stated that digital surveillance may engage a state's human rights obligations extraterritorially, regardless of the nationality or location of individuals whose communications are under surveillance.[1]

[1] A/HRC/27/37, paras. 31-36.

DRIPA also enables the government to require telephone and internet companies in the UK and abroad to collect metadata on their customers' communications and store it for up to 12 months. The Act was presented to parliament over three months after the Court of Justice of the European Union (CJEU) ruled that blanket data retention is disproportionate and breaches the right to privacy.

The new law fails to address the concerns raised by the CJEU in its ruling, and goes further than the regulations it is purported to replace by expanding the government's surveillance powers extraterritorially. Indeed the new Act subjects a range of internet and telecommunications companies outside the UK to orders for intercepting the content of communications.

The OHCHR's July 2014 report specifically states that the mere collection of metadata can interfere with the right to privacy, even if it is not subsequently viewed or used. The report also stated that mandatory, blanket third-party data retention "appears […] neither necessary nor proportionate" (para 26).

The need for independent oversight and transparency

The government should create a more robust, independent and transparent oversight authority that reports to Parliament on the government's surveillance activities. This authority should be mandated to disclose as much information to the public as possible, consistent with the need to redact information necessary to protect legitimate national security or public order interests.

Human Rights Watch believes that the existing oversight and accountability mechanisms in this area are not adequate to prevent abuse of surveillance powers, and are not consistent with the UK's human rights obligations, in particular the obligation to protect the right to privacy.

Oversight under RIPA is neither transparent nor comprehensive. The interception of communications commissioner has oversight of the government's power to intercept, but the prime minister, not the parliament, appoints the commissioner, thereby compromising the independence of the position. The commissioner examines a number of interception warrants after the fact and assesses whether they comply with the criteria of necessity and proportionality. The commissioner's 2014 annual report—for which the prime minister must approve the content—states that a random sample of around 10 percent of applications for warrants submitted by larger users such as police forces are inspected.

The OHCHR's report on privacy in the digital age states that oversight of surveillance programs by all branches of government as well as an independent civilian agency is essential to ensure effective protection of law (para. 37).

Those whose communications are the object of an interception warrant are not notified that they are under surveillance. A person who believes one of the intelligence agencies has breached their right to privacy through surveillance can file a complaint before the

Investigatory Powers Tribunal, a judicial body made up of judges and lawyers. The tribunal can quash the interception warrant and order the records collected to be destroyed or award compensation. If the tribunal rejects a person's claim, it doesn't let the person know whether an interception took place. The tribunal's decisions are not subject to appeal or judicial review.

In accordance with the right to an effective remedy under Article 13 of the ECHR and Article 2 of the ICCPR, individuals who are subject to a surveillance warrant should be given enough time and information about the decision to put their communications under surveillance to allow them to challenge the decision effectively before a court, and they should have a right of appeal. Notice can be delayed in certain circumstances, including where advance notice would seriously jeopardize the legitimate purpose of the surveillance. However, notice after the fact is important for enabling redress where abuses occur.

Furthermore, the government should ensure that the measures it announced in July, including a new Privacy and Civil Liberties Oversight Board (PCLOB) based on the US model are implemented in a way that enables effective oversight and public scrutiny of UK government surveillance practices. In order to be effective, such a mechanism should be fully independent from the government and its agencies and not report to any other authority; it should have sufficient resources to conduct effective and comprehensive oversight and it should have the power to obtain any evidence it requires to carry out its functions. The new mechanism should also be mandated to oversee surveillance of "external" as well as "internal" communications subject to surveillance by the UK government, whether the person whose communications are intercepted is based in the UK or abroad. The annual transparency reports on how surveillance powers operate, also announced by the government in July, should reveal as much information to the public as possible in a way that is consistent with national security and public order.

Reports on reviews of government surveillance should also be public and transparent to the extent possible. Human Rights Watch is concerned that under section 7(6) of the Data Retention and Investigatory Powers Act 2014, parts of the public version of the Investigatory Powers Review's report may be excluded by the Prime Minister on the grounds that they are "contrary to the public interest or prejudicial to national security." Human Rights Watch holds that the decision on what should be redacted from the public version should be taken by the independent reviewer, not the Prime Minister. Redactions should also be limited to only what is truly necessary to protect legitimate national security interests or prevent or detect serious crime. Similarly, we are concerned that the Prime Minister approves the content of the Interception of Communications Commissioner's annual report before it is made public. Under section 58(7) of RIPA, the Prime Minister can exclude parts of the report on broad grounds, for instance that publication would be "contrary to the public interest" or that it would be prejudicial to national security, "the prevention or detection of serious crime," "the economic well-being of the United Kingdom" or "the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Commissioner." Redactions should be instead

limited to only what is truly necessary to protect legitimate national security interests or prevent or detect serious crime.

For more information, please see:

Joint Civil Society Statement on Privacy in the Digital Age, Submitted to the 27th session of the UN Human Rights Council (September 2014)
http://www.hrw.org/node/129031
Submission to the UN Human Rights Committee on Concerns and Recommendations on the United Kingdom (July 2014)
http://www.hrw.org/news/2014/07/31/submission-un-human-rights-committee-concerns-and-recommendations-united-kingdom
United Nations: Rein in Mass Surveillance (press release, July 2014) http://www.hrw.org/news/2014/07/17/united-nations-rein-mass-surveillance
UK: Emergency Surveillance Law a Blow to Privacy (press release, July 2014) http://www.hrw.org/news/2014/07/14/uk-emergency-surveillance-law-blow-privacy
A Clear-Eyed Look at Mass Surveillance (op-ed by Cynthia Wong, July 2014)
https://www.opendemocracy.net/opensecurity/cynthia-wong/cleareyed-look-at-mass-surveillance-0
The UK's Mass Surveillance Confirmed – Finally (dispatch, June 2014) http://www.hrw.org/news/2014/06/19/dispatches-uk-s-mass-surveillance-confirmed-finally
UK: Do Not Make Us Choose Between Our Safety and Our Privacy (op-ed by Izza Leghtas, June 2014) http://www.hrw.org/news/2014/06/04/uk-do-not-make-us-choose-between-our-safety-and-our-privacy
Submission to the UK's Intelligence and Security Committee of Parliament – Privacy and Security Inquiry (February 2014)
http://www.hrw.org/news/2014/03/10/submission-uk-s-intelligence-and-security-committee-parliament-privacy-and-security-
UK Should Come Clean About Surveillance (dispatch, October 2013)
http://www.hrw.org/news/2013/10/31/dispatches-uk-should-come-clean-about-surveillance
UK: Provide Clear Answers on Data Surveillance (press release, June 2013) http://www.hrw.org/news/2013/06/28/uk-provide-clear-answers-data-surveillance

Interception of Communications Commissioner's Office

Contents

1. Introduction

1.1 During the debates considering the Data Retention and Investigatory Powers Bill, the Home Secretary announced to Parliament that the Reviewer of Counter-terrorism Legislation[1] is to lead a review before the General Election, of -

- the capabilities and powers required by law enforcement and the security intelligence agencies; and,
- the regulatory framework within which those capabilities and powers should be exercised.

1.2 This paper is the written contribution from the Interception of Communications Commissioner's Office (IOCCO) to the review.

1.3 We propose to comment on the following areas of policy -

- the effectiveness of the current statutory oversight arrangements;
- safeguards to protect privacy;
- the case for amending or replacing legislation.
- statistical and transparency requirements that should apply.

1.4 We have sought to draft this paper in plain language to make it accessible to any person with an interest in the subjects being discussed. However, this paper sets out our observations about the law relating to the interception of communications, the retention, acquisition and disclosure of communications data and how this intrusive material is used once obtained. Inevitably, some legal and technical language has been used but we have tried our very best to properly explain the cause and effect.

1.5 Finally, thank you to the Independent Reviewer for allowing IOCCO extra time to finalise our submission.

[1] See https://terrorismlegislationreviewer.independent.gov.uk/

2. Effectiveness of current statutory oversight arrangements

2.1 The creation of the oversight regime

2.1.1 The debates in Parliament in March 2000, considering the then Regulation of Investigatory Powers Bill, are a good starting point in which to contextualise the current workings of the Regulation of Investigatory Powers Act 2000 ("the Act") and the oversight process. Parliament greatly expanded the role of the Interception of Communications Commissioner[2] ("the Interception Commissioner") from what was initially set out in earlier law, the Interception of Communications Act 1985, which was limited to conduct by the few agencies and relating only to interception.

2.1.2 The introduction of the Act set a legal process for the acquisition and disclosure of communications data by public authorities[3] within the United Kingdom that Parliament determined should be able to undertake the acquisition of communications data -

> Standing Committee F - Tuesday 28 March 2000 Regulation of Investigatory Powers Bill
>
> Comments by the Minister of State, Home Office (Mr. Charles Clarke):
>
> *"At present, the Data Protection Act safeguards are fairly lax, and have been made tighter only through voluntary co-operation between the telecoms industry and law enforcement. There is currently no independent oversight. The Bill places oversight of the use of this power under the remit of the interception of communications commissioner, which will give greater guarantees to the citizen than those that exist under the present arrangements".*

[2] See section 8 of the Interception of Communications Act 1985

[3] See the Regulation of Investigatory Powers (Communications Data) Order 2010 which contains a list of the public authorities able to use these powers, the ranks of the persons designated to grant access and the various types of communications data they may acquire http://www.legislation.gov.uk/ukdsi/2010/9780111490341/pdfs/ukdsi_9780111490341_en.pdf

2.1.3 The Act therefore replaced a disclosure process that was undertaken under the Data Protection Act 1998 and which was administered through a series of non-statutory agreements between the various communication service providers (CSPs) and the public authorities, which included police forces, law enforcement and intelligence agencies, government departments with particular investigatory responsibilities and local authorities whose functions include those of trading standards.

2.1.4 As indicated in the debate, disclosures under the Data Protection Act 1998 did not have an oversight process and the safeguards were fairly lax; so the purpose of Chapter 2 of Part 1 of the Act was to regulate access to communications data, not to extend it[4].

2.1.5 The role of the Interception Commissioner and his Inspectors from the Interception of Communications Commissioner's Office (IOCCO) is to perform an audit. The use of the terms oversight or overseer, often applied to our role, are somewhat misleading and do not best describe what Parliament intended or what we are required to do in practice.

> Standing Committee F - Tuesday 28 March 2000 Regulation of Investigatory Powers Bill
>
> Comments by the Minister of State, Home Office (Mr. Charles Clarke):
>
> *"An audit team from the commissioner's office will undertake periodic inspections of each body to ensure that the power is being used responsibly. [.....]. The teams will inspect records, checking the details to ensure the necessity and proportionality of what has been requested".*

[4] See 2003 consultation paper "Access to Communications Data – Respecting Privacy and Protecting the Public from Crime" - page 10

"I used the term "audit teams'' to establish that an audit will check what is happening in practice, rather than examine every case universally. We do not anticipate the need for a substantial apparatus to carry out that task. However, we do anticipate that proper regimes, such as audits, will be put in place to check that procedures are being properly followed. We shall then be able to make judgments about the necessity and proportionality of what is being done. I should like to put the right hon. Gentleman's mind at rest about the scale of the operation. I used the word ``audit'' because we want to establish systems that will genuinely assess what is taking place".

"I wanted to lay to rest the idea that we might introduce some great bureaucratic operation, and to explain why I used the word "audit'' rather than specifying a universal method of checking".

2.1.6 We have developed those audits over the years and they are now at a significantly more mature level. Further comment is made on our audits later in this paper. Our capability has also been enhanced through our recruitment of four additional Inspectors in 2013 and 2014.

2.2 Our role within the current statutory oversight arrangements

2.2.1 The Act[5] provides for an Interception Commissioner whose remit is to provide independent oversight of the exercise and performance of the powers and duties contained under Chapter 1 (interception) and Chapter 2 (acquisition and disclosure of communications data) of Part 1 of the Act. The Interception Commissioner is now supported by a team of ten inspectors (including the Head of IOCCO) and two secretariat.

[5] See sections 57 & 58 of the Act

2.2.2 We have published information about who we are on our website[6] to enable the public to have more information about the Interception Commissioner, his team, and more importantly what we actually do –

- inspections of the nine agencies (intelligence and law enforcement agencies) who may undertake the interception of communications under an interception warrant and the four warrant granting departments[7];
- inspections of all relevant public authorities who are authorised to acquire communications data[8];
- the investigation of unintentional electronic interception (not related to trying to put into effect an interception warrant). The European Commission identified deficiencies in the way in which the Data Protection Directive and the E-Privacy Directive were transposed. As a result, the offence of unintentional electronic interception, which attracts a civil penalty, was added[9]; and,
- inspections of the interception of communications in prisons in England, Wales and Northern Ireland by non-statutory agreement. This is lawful under section 47 of the Prison Act 1952 or section 13 of the Prison Act (Northern Ireland) 1953 (prison rules) – see section 4(4) of the Act.

2.2.3 It is the duty of every person to comply with any request made by the Commissioner and to disclose or provide to the Commissioner all such documents and information as he may require carrying out his functions – see section 58(1) of the Act. This means we have full and unrestricted access to all of the information, systems and documents that we need.

[6] See http://iocco-uk.info/sections.asp?sectionID=9&type=top

[7] See Paragraphs 3.3 and 3.30-3.33 of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

[8] See Annex A of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

[9] See http://iocco-uk.info/sections.asp?sectionID=2&chapter=6&type=top for moreinformation

2.2.4 To carry out our functions we maintain a strategic relationship with the Communication Service Providers (CSPs) which greatly assists us to carry out thorough inspections of the requirements made of them by public authorities concerning the acquisition and disclosure of communications data and their ability to comply with warrants relating to the interception of the content of communications.

2.2.5 We also maintain a close liaison with the communications data Single Points of Contact[10] (SPoCs) within public authorities who perform a guardian and gatekeeper role ensuring that the public authorities act in an informed and lawful manner when acquiring communications data. In practice our relationships with the SPoCs and CSPs serve us well.

2.3 Examination of systems and procedures for the interception of communications

2.3.1 Our interception inspections are structured to ensure that key areas derived from Chapter 1 of Part 1 of the Act and the Code of Practice are scrutinised. A typical inspection may include the following:

- a review of the action points or recommendations from the previous inspection and their implementation;
- an evaluation of the systems in place for the interception of communications to ensure they are sufficient for the purposes of the Chapter 1 of Part 1 of the Act and that all relevant records have been kept;
- examination of selected interception applications to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;

[10] See Paragraphs 3.15 to 3.21 of the Acquisition and Disclosure of Communications Data Code of Practice for more information on the role of SPoC.

- interviewing case officers, analysts, linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;
- examination of the urgent oral approvals to check the process was justified and used appropriately;
- an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data;
- a review of the errors reported, including checking that the measures put in place to prevent recurrence are sufficient;
- any inquiries as directed by the Interception Commissioner. For example, in 2013 we conducted investigations into matters raised by media disclosures related to revelations stemming from Edward Snowden.
- the compilation of a detailed inspection report and action plan setting out the findings, recommendations and overall level of compliance. This is sent to the head of the relevant interception agency with a copy for the relevant Secretary of State.

2.3.2 In 2013 our office carried out 26 interception inspections. During the inspections we examined 600 interception warrants. This represents just over one third of the extant warrants at the end of the year and one fifth of the new warrants issued during the year. The total number of recommendations made during our interception inspections in 2013 was 65, an average 7 recommendations for each interception agency. More detailed information on our interception work can be found in our 2013 Annual Report[11].

[11] See Section 3 of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

2.4 Examination of systems and procedures for acquiring communications data

2.4.1 Our communications data inspections are structured to ensure that key areas derived from Chapter 2 of Part 1 of the Act and the Code of Practice are scrutinised. A typical inspection may include the following:

- the supply of a pre-inspection pack (two months prior to our visit) to the head of the public authority to require information and arrange interviews with operational teams;
- a review of the action points or recommendations from the previous inspection and their implementation;
- an audit of the information supplied by the CSPs detailing the requests that public authorities have made for disclosure of data. This information is compared against the applications held by the Single Point of Contact (SPoC)[12] to verify that the necessary approvals were given to acquire the data (more on this below);
- random examination of individual applications for communications data to assess whether they were necessary in the first instance and then whether the requests met the necessity and proportionality requirements;
- query based examination of applications, via interrogation of the secure auditable computer systems used by the larger public authorities, to identify trends, patterns and compliance issues in key parts of the process across large volumes of applications (more on this below);
- scrutinising at least one investigation or operation from start to end to assess whether the communications data strategy and the justifications for acquiring all of the data were proportionate;
- examination of the urgent oral approvals to check the process was justified and used appropriately;

12 See Paragraphs 3.15 to 3.21 of the Acquisition and Disclosure of Communications Data Code of Practice for more information on the role of SPoC

- a review of the errors reported or recorded, including checking that the measures put in place to prevent recurrence are sufficient;
- any inquiries as directed by the Interception Commissioner. For example, we are in the process of conducting investigations into whether there might be institutional overuse of the powers by police forces, and, the acquisition of data to identify journalistic sources; and,
- the compilation of a detailed inspection report and action plan setting out the findings, recommendations and overall level of compliance. This is sent to the head of the relevant public authority, i.e. the Chief Constable or Chief Executive.

2.4.2 In 2013 our office conducted 75 communications data inspections. An additional 130 local authorities were inspected via the National Anti Fraud Network (NAFN) who provides a SPoC service for local authorities. In 2013, 85% of the local authorities using their powers submitted their requirements via the NAFN SPoC.

2.4.3 The length of each inspection depends on the type of public authority being inspected and their communications data usage. The inspections of the larger users, such as police forces, are conducted by at least two inspectors and take place over 3 or 4 days. The inspections of the smaller volume users are conducted by one inspector and generally last 1 day. The total number of recommendations made during our communications data inspections in 2013 was 299. More detailed information on our communications data work can be found in our 2013 Annual Report[13].

2.4.4 On a regular basis the CSPs share with us information generated by the secure auditable systems that manage their disclosures to requirements made under the Act. Those audit systems contain information such as the name of the public authority acquiring data, the URN of the request, the data description and the

[13] See Section 4 of our 2013 Annual Report for more information http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

statutory purpose used. This information allows our inspectors to perform a back audit when inspecting public authorities to assess whether there is a corresponding authority in place and its scope.

2.4.5 We also have direct engagement with the software companies that supply secure auditable systems for administering communications data applications in the majority of the police forces and law enforcement agencies (who between them account for nearly 90% of the communications data requests). The software companies have developed capabilities to enable our inspectors to retrieve data by means of query based searches relating to the applications and authorisations so as to give better insight into all of the activities undertaken by an authority. This enables specific areas to be tested for compliance, and, trends and patterns to be identified from the extraction of information from large volumes of applications, for example –

- extraction of named designated persons (DPs) and their recorded considerations for each application to check they are discharging their statutory duties responsibly, i.e. that they are not rubber stamping applications, that they are of the appropriate rank or level to act in that capacity, that they are independent of the investigation or operation;
- requests where service use or traffic data has been applied for over lengthy time periods to check relevance and proportionality;
- the acquisition of particularly intrusive data sets to examine the proportionality and intrusion considerations balanced against the necessity.

2.4.6 An application for communications data, and whether it is necessary and proportionate, is considered on the content of the application at the time it is considered by the DP determining whether to authorise it. It is our post-authorisation or down-stream audit of what is (or just as importantly what is not) being done with the data that makes our inspections unique in bringing about more scrutiny and oversight of the process. We discuss this point in more detail in the section of this paper considering prior judicial approval.

3. Safeguards to protect privacy

In addition to the oversight by the Interception Commissioner and audit by IOCCO there are other dimensions to the safeguards that we are well placed to, and therefore should, contribute to in one way or another and we will do so in this section. Reflecting on the current oversight arrangements and the safeguards has caused us to revisit some of the basic elements of the Act. We now set out our observations about what works and, in an operational sense, what does not.

3.1 The right to effective remedy - Investigatory Powers Tribunal

3.1.1 The European Convention of Human Rights ("the Convention") has had various amendments and additions made to it over the years. Article 13 of the Convention relates to the Right to an Effective Remedy -

> *Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.*

3.1.2 The Human Rights Act 1998 (HRA) does not include Article 13 relating to the Right to Effective Remedy. We understand that at the time of enactment of the HRA the view taken was that citizens within the United Kingdom would be able to seek a remedy by pursuing an action through the civil or criminal court in relation to any breach of the Convention. There have been amendments to HRA since the initial implementation (for example the withdrawal by the United Kingdom of its derogation from the Convention which concerned the detention provisions in the Anti-terrorism, Crime and Security Act 2001) but Article 13 remains absent from the HRA.

3.1.3 The Act at section 65 sets out the role and responsibilities of the Investigatory Powers Tribunal ("the Tribunal"). The section makes explicit it is the

Tribunal that is the appropriate forum if it is a complaint from a person who is aggrieved by conduct such as the interception of their communications or the acquisition of their communications data and which a person believes to have taken place in relation to them.

3.1.4 The references to a threshold for complaints dealt with by the Tribunal in the Act appears at section 65(4) and states a person needs to be "……aggrieved by any conduct……" and section 67(4) states a Tribunal does not have to hear complaints that are "……frivolous or vexatious……" and section 65(5) indicates complaints must be relating to conduct within 1 year of the conducts occurrence. In practice, the effect is –

- the complaint to the Tribunal must be from the person aggrieved;
- a third party, such as the Interception Commissioner, IOCCO or a CSP, appear unable to have their reports acted upon by the Tribunal, as the Tribunal appear limited, in law, to respond only to a complaint from the person aggrieved;
- in practice it will be virtually impossible for the aggrieved person to ever be aware of the interception of communications due to the requirement to keep secret matters relating to the existence of a warrant and the exclusion of the product of warranted interception from legal proceedings;
- there may be circumstances when communication data may be challenged as to its admissibility in criminal trials but this does not equate to matters dealt with by the Tribunal;
- section 65(5) indicates complaints must be relating to conduct within 1 year of the conduct's occurrence; and,
- the Tribunal processes appear to deal with the actions of public authorities and therefore it is not clear if that would include investigating the circumstances when a CSP is at fault concerning the interception of the wrong communications address and / or the disclosure of the wrong communications data. In 2013 we reported that 20 percent of the

interception errors and 12.5 percent of the communications data errors were caused by CSPs.

3.1.5 The code of practice accompanying Chapter 2 of Part 1 of the Act relating to the acquisition and disclosure of communications data (at paragraph 8.3) states –

> "*Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal".*

3.1.6 The threshold set out in the code of "……*individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers"* where it relates to the acquisition of communications data appears artificial as the Act creates no such threshold to engage the Tribunal. The code also appears to confirm that erroneous actions are restricted to those of public authorities and do not include the actions of CSP when things go wrong.

3.1.7 In practice, it is the Interception Commissioner and IOCCO who will be in possession of the information as the result of the initial inspection process and, when appropriate, through the use of the powers within section 58(1) requiring the disclosure of additional information. The consequence in practice; if IOCCO becomes aware that, for example, a police force has misused their powers to acquire communications data then the proposed course of conduct suggested in the code of practice (at paragraph 8.3) of informing the aggrieved person is a rare possibility as informing them may alert them about the investigation / operation which might

amount to an act of 'tipping off', and, may be detrimental to a successful investigation or conflict with national security requirements[14].

3.1.8 Where interception with a warrant is concerned the Act prohibits an individual from being informed that their communications have been intercepted in circumstances that if they were made aware they may seek to engage the Tribunal. The code of practice accompanying Chapter 1 of Part 1 of the Act concerning the interception of communications makes no mention of the Tribunal or its processes.

3.2 The definition of content and communications data

3.2.1 The definition of communications data has not changed since the Act came into existence, despite the fact that communications technologies, and thus the types of information generated and processed have changed dramatically.

3.2.2 Section 81(1) of the Act defines a communication to include anything comprising of speech, music, sounds, visual images or data of any description. It also includes the movement of those communications between persons, a person and a thing or between things. So, that would include an end-user downloading music from a website and sharing it with other users via a telecommunication system. It also includes the actuation or control of another apparatus within a telecommunication system for example, activating storage from one device to another device via a telecommunication system.

[14] See **DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** of 25 November 2009 amending **Directive 2002/22/EC** on universal service and users' rights relating to electronic communications networks and services, **Directive 2002/58/EC** concerning the processing of personal data and the protection of privacy in the electronic communications sector and **Regulation (EC) No 2006/2004** on cooperation between national authorities responsible for the enforcement of consumer protection laws and in particular see recital (or paragraph) 64 -
"In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of the breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law enforcement authorities in cases where early disclosure could unnecessarily hamper the investigation of the circumstances of a breach."

3.2.3 In practice users will often access several telecommunication services via their mobile phone and those services are unlikely to be supplied by the CSP who provides their network connection. Put simply, service use and traffic data are the data generated and processed by the CSP who provides network access; and other providers of telecommunication services accessed via a network connection.

3.2.4 The definitions of service use and traffic data (see sections 21(4)(a) & (b) & section 21 (6)) of the Act are, in our view, still generally fit for purpose, albeit they can be difficult to understand without proper explanation especially when a new product is launched by a CSP i.e. which definitions apply and when. Hopefully the following paragraphs can assist to explain some of the pressing issues in this regard.

3.2.5 The recent developments of communications technology appear to be included within the current definitions of service use and traffic data and an update to the examples in the Chapter 2 of Part 1 Code of Practice needs to incorporate some more recent developments as working examples.

3.2.6 One area that does need significant attention is the ability to determine what constitutes the content of a communication within the online environment. The Act refers to content several times but content itself is never defined in the Act. Explanations, therefore, that seek to differentiate by giving a threshold of, for example, "nothing beyond the first slash" do not take account of the developments within the Internet environment (for example social media), and are, in reality not best understood by investigators or CSPs managing disclosures. By way of explanation -

http://iocco-uk.info/ is said to be communications data – i.e. "nothing beyond the first slash" whereas the following link - https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/ (which is the log-in webpage to activate access to webmail) goes well

beyond the 'first slash' and may, at first appearance, be considered to be content of a communications.

3.2.7 However, section 21(6)(b) explains that traffic data (defined in section 21(4)(a)) may include data identifying or selecting or purporting to identify or select, apparatus through which, or by means of which, the communications is or may be transmitted. This then begs the question whether the log-in webpage (no matter how many 'slashes' there are within the web addresses) is communications data or the content of a communication. Amendments to the Act need to be undertaken to define what is content and by doing so better determine that which the term communications data relates to when generated within the online environment.

3.2.8 The volumes and detail contained, especially in traffic data, are at a level not envisaged in 2000. The introduction of mobile phone networks with capacity to be able to provide access to radio & television channels, social networking and other services is staggering and so is the volume and detail of the data generated as a result, especially relating to the location of a mobile phone / end user device.

3.2.9 At the time the RIP Bill was being debated in 2000, traffic data relating to the location of a mobile telephone (commonly referred to as cell-site data) indicated the cell-site linked to telephone calls and text messages. The data retention requirements developed some 8 years ago required CSPs to retain cell-site data relating to telephone calls and text messages.

3.2.10 Communications data that may be used to determine the whereabouts of a mobile phone / end user device within a network is now made up by 3 elements -

1) cell-site data associated to voice and SMS retained by the mobile CSP (as described above);
2) cell-site data associated to the mobile data access channel (aka 3G or GPRS) which may relate to social media updates, messaging, access to a television channel etc.

3) Wi-Fi data indicating specific locations (for example food outlets, transport hubs such as railway stations, service stations etc) the data for which might be retained by the mobile CSP and / or another national or local provider as part of another service (for example a hotel, tube station, airport lounge, transport carrier, shopping mall, coffee shop, restaurant etc.).

3.2.11 The amount of information collected by the provider of a communications service about the people to whom they provide a service has also increased considerably and this means that the definition of "subscriber information" potentially now covers a wider catchment of data than originally available.

3.2.12 Subscriber information means, within section 21(4)(c), information held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person that is not service use data and not traffic data. When the Act was being developed some fifteen years ago subscriber data meant little more than for example, the name of the account holder, the billing postal address, the installation address of the landline, other telephone numbers present on the account.

3.2.13 The communications industry now collects significant amounts of information about the people to whom they provide pre-pay, post-pay and more latterly free or unsubscribed services. It is best to distinguish the data collected about those persons (subscriber information) from the data the industry generate or process as part of their technical infrastructure, and note that subscriber information simply means anything the CSP collects about their customer that is not data generated by the network nor is it data within their billing systems. Customers are encouraged to manage their accounts via on-line portals / 'Apps'[15] and are likely to disclose a whole

[15] "Apps" – software applications designed to run on end user devices to perform certain tasks or give streamlined access to telecommunication services (such a messaging) or information (such as weather reports).

range of personal data, for example, their viewing preferences for online media, sexual preferences, political or religious associations etc.

3.3 Authorised access to communications data

3.3.1 The offices, ranks or positions of the Designated Persons (DPs) who grant access to communications data are listed in the Regulation of Investigatory Powers (Communications Data) Order 2010[16]. The prescribed DPs who can authorise access to subscriber data (of such detail described in the previous section), not envisaged by Parliament, is worthy of consideration because of the degree of 'privacy intrusion' within subscriber information and the risk of identifying details of an individual's life, behaviour, beliefs, that the individual might regard as being more intrusive than a list of the communications that they have made or received.

3.3.2 Furthermore, the fact that some public authorities have one level of DP to authorise different types of communications data under section 21(4), whereas others have a higher ranking DP prescribed for what are traditionally thought of as the more intrusive data sets ought to be reviewed, not least to ensure the ranks / levels are comparative across the various public authorities. For example, in local authorities a DP can authorise subscriber information or service use data if they are a Director, Head of Service, Service Manager or equivalent. Similarly in the Gambling Commission one level of DP (a Head of Department) can approve all types of communications data (subscriber information, service use data and traffic data). Whereas in a police force, an Inspector can approve subscriber information, but, service use and traffic data, traditionally thought of as more intrusive data sets, must be considered by a higher ranking officer, a Superintendent.

[16] See the Regulation of Investigatory Powers (Communications Data) Order 2010 which contains a list of the public authorities able to use these powers, the ranks of the persons designated to grant access and the various types of communications data they may acquire http://www.legislation.gov.uk/ukdsi/2010/9780111490341/pdfs/ukdsi_9780111490341_en.pdf

3.4 Interception error reporting provisions

3.4.1 There is no provision for error reporting or definition of an error in the Interception of Communications Code of Practice. This leaves the interception agencies and our office struggling with an ill-defined framework. We are satisfied that there is still a good culture of self reporting, however in 2013 we reported that our investigations had identified a lack of consistency in relation to the types of error instances that are reported. This is because different thresholds and judgments are applied by each interception agency.

3.5 The role of the Single Point of Contact (SPoC)

3.5.1 We are the only Member State within the EU that has a SPoC system for acquiring communications data – accredited individuals who are trained to an expert level in acquiring the data. The SPoC's provide a guardian and gatekeeper function and ensure that their public authority acts in an informed and lawful manner when acquiring communications data. The CSP's can refuse to comply with a notice or withdraw agreement concerning an authorisation if the conduct to acquire the data does not involve a SPoC. This system ensures that data is only required when a lawful request has been made and that the data is disclosed to a known contact within the public authority.

3.5.2 The role of the SPoC and the safeguarding function they perform is set out in the Code of Practice which accompanies Chapter 2 of Part 1 of the Act. This important safeguard is not prescribed in the Act itself. The role of those working as SPoCs needs to be included in the Act, amplified in a revised Code of Practice and further enhanced by the publication professional minimum competencies by the Home Office and College of Policing.

3.6 Requirements for CSPs to retain communications data

3.6.1 There does not appear to be a legal requirement for the Interception Commissioner or any other independent oversight body to review the implementation of section 1 of the Data Retention and Investigatory Powers Act (DRIPA) which relates to the giving of notice by a Secretary of State requiring the retention of specific communications data by a CSP. There is currently no means of redress (i.e. Tribunal) for a CSP should they consider a notice requiring the retention of communications data is or has become disproportionate and should be cancelled, and, there has been a refusal to cancel it.

3.6.2 There does not appear to be a legal requirement for the Interception Commissioner or any other independent oversight body to review whether DRIPA widens the retention requirements when compared to the Data Retention (EC Directive) Regulations 2009 which it replaced[17]. The potential widening effect of DRIPA was an area of concern expressed during the debates in Parliament.

3.7 Non-compliance in relation to requirements to intercept communications or disclose data

3.7.1 Statutory oversight, audit and where appropriate, investigation, is undertaken by IOCCO when CSPs intercept communications or disclose their communications data under the Act and this includes circumstances when they disclose in error.

3.7.2 We do not oversee, audit or report to the Prime Minster when CSPs fail or refuse to intercept communications or disclose communications data when a lawful requirement is made of them within the Act.

[17] See http://iocco-uk.info/docs/IOCCO%20response%20to%20new%20reporting%20requirements.pdf for our full response to DRIPA.

3.7.3 This is a concern now that section 4 of DRIPA amends Part 1 of the Act and makes explicit the extra-territorial reach in relation to both the interception of communications and the acquisition of communications data by adding specific provisions. The amendments to the Act introduced by DRIPA confirms that requirements for interception and the acquisition of communications data to overseas companies that are providing communications services within the United Kingdom are subject to the legislation.

3.8 The use of other powers to acquire communications data

3.8.1 Chapter 2 of Part 1 of the Act appears to provide an exclusive scheme whereby communications data can be obtained. This is reinforced by section 21(1) which states that the Chapter applies to 'any conduct' in relation to obtaining of communications data, and to the disclosure to 'any person' of such data. The approach appears consistent with paragraph 1.3 of the Code of Practice for the Acquisition and Disclosure of Communications Data, which states:

> *"Relevant public authorities for the purposes of Chapter 2 of Part 1 of the Act should not:*
>
> - *Use other statutory powers to obtain communications data from a postal or telecommunications operator unless that power provides explicitly for obtaining communications data, or is conferred by a warrant or order issued by the Secretary of State or a person holding judicial office, or [emphasis added]*
>
> - *Require, or invite, any postal or telecommunications operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998."*

3.8.2 In plain language that means public authorities should not use other laws to obtain communications data from a postal or telecommunications operator unless that law provides explicitly for obtaining communications data.

3.8.3 Parliament recently reinforced those restrictions within the Data Retention and Investigatory Powers Act 2014 (DRIPA) at section 1(6)(a) which puts a duty on the CSP not to disclose communications data retained as a result of a requirement within section 1 of DRIPA unless it is a requirement made under Chapter 2 of Part 1 of the Act; or a court order or other judicial authorisation or warrant.

3.8.4 However, there are numerous other laws which give general information powers or provide explicit powers for obtaining communications data (such as the Social Security and Fraud Act 2001 and the Social Housing Fraud Act 2013) and cases where the data retained by the CSP is not subservient to a section 1 DRIPA requirement (for example, records a CSP has determined they need to retain as part of their business function).

3.8.5 The Protection of Freedoms Act 2012[18] requiring local authorities to seek judicial authority for communications data was implemented in November 2012. The Government, in the following year, implemented the Social Housing Fraud Act 2013 which gave provision for the acquisition of service use data and subscriber information in circumstances when the data may assist to investigate housing fraud without a requirement to gain judicial approval. The Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 allows the local authority, not Parliament, to pick which local authority employees can authorise access to the data and determine what restrictions may apply to their actions, see the "Safeguards" in the Regulations –

- *"Requests for data could only be made by an authorised officer – someone who is a local authority employee and who has been authorised by the local authority's Chief Executive or Chief Finance Officer to make requests."*

[18] Protection of Freedoms Act 2012 ttp://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

- *"A local authority would be able to impose any restrictions it wished on its authorised officer and be able to withdraw authorisation at any time."*

3.8.6 The result is a two tier process in operation within the United Kingdom when there is a need for a local authority to undertake the acquisition of communications data. For example, in circumstances where a citizen is an elderly person defrauded by a rogue trader – Trading Standards must go through the rigours set down by Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act; the accompanying code practice; the additional requirements imposed by the Protection of Freedoms Act (requiring the local authorities to seek judicial approval); and subject to oversight by IOCCO. But where the local authority is subject to fraud they can investigate a crime against themselves and do not have to comply with such rigours.

3.8.7 We are of the view that CSPs should not required by law to obtain and disclose communications data other than in cases where the relevant statutory framework expressly guarantees the substantive protections of Article 8 and Directive 2002/58/EC (Directive on privacy and electronic communications).

3.8.8 We do not oversee, audit or report to the Prime Minster the use of other laws to acquire communications data which allow the public authorities using them to engage directly with the CSPs without the use of a SPoC. The person authorising is often of lower office (rank or level) and does not have to be independent from the investigation or operation; and there is no means of redress via the Tribunal.

3.8.9 Furthermore we do not oversee, audit or report on any errors or wrongful disclosures resulting from the acquisition of data using other powers.

3.9 The use of other powers to access the content of stored communications

3.9.1 Section 2(1) of the Act defines a telecommunication system as any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. "Apparatus" for these purposes includes any equipment, machinery or device and any wire or cable.

3.9.2 Sections 2(7) and (8) explain how a communication that is being stored within a telecommunication system for the intended recipient to gain or regain access to it is said to be in the course of its transmission (for example, voicemail messages stored by the CSP). Expressed another way, stored communications are always in the course of transmission even if the intended recipient has accessed them[19]. The consequence is that stored communications have the protection of section 1 of the Act which creates a criminal offence of unlawful access.

3.9.3 Accessing the content of stored communications held by a CSP will have lawful authority under section 1(5) of the Act if it is either –

- in accordance with an interception warrant under section 5 of the Act, or,
- in exercise of any statutory power that is exercised for the purpose of obtaining information or of taking possession of any document or property.

3.9.4 Reference within section 1(5)(c) to a statutory power will include the use of a section 9 Police and Criminal Evidence Act (PACE) order-

> Standing Committee F - Tuesday 16th March 2000 Regulation of Investigatory Powers Bill
>
> Comments by the Minister of State, Home Office (Mr. Charles Clarke):

[19] See also R v Edmondson, Brooks & others [2013] EWCA Crim 1026

> ".....Where a communication already exists, clause 1(5)(c) would allow the police to obtain a production order for access, but future communications must be accessed through an interception warrant....."

3.9.5 CSPs now deal with significant volumes of judicial orders made under section 9 of PACE (and similar) requiring the disclosure of voicemails, text messages, information retained within online storage systems, and emails. This is conduct that was envisaged by Parliament. The Times newspaper, in an article on 20th October 2014[20], revealed that one mobile CSP was receiving 150 such requirements per month. The article made the point -

> ".....Unlike warrants for eavesdropping on live conversations, so called production orders need only the approval of a judge.....", ".....the data is stored and is available to police with a production order obtained from a judge after campaigners fear is often cursory deliberation....."

3.9.6 We can confirm there is currently no oversight or audit by IOCCO of the use of other powers to acquire stored communications (for example by way of section 9 PACE orders). Furthermore there is no oversight of any errors or wrongful disclosures resulting from the use of such other powers.

3.10 The use, retention, storage and destruction of communications data within public authorities

3.10.1 We instigate thorough audits of the processes in place for the retention, storage and destruction of intercepted material and related communications data under Chapter 1 of Part 1 of the Act, but, we have no statutory footing upon which to intervene in matters relating solely to the retention, storage, processing, and destruction of communications data acquired under Chapter 2 of Part 1 of the Act within public authorities.

[20] http://www.thetimes.co.uk/tto/news/uk/article4241503.ece

3.10.2 Our inspections confirm to us how revealing, informative and, as a consequence, highly intrusive interception and communications data are in the hands of a skilled investigator. This is balanced against the very important role the prompt and efficient interception of communications or acquisition of communications data, and, the consequent analysis plays to save life, thwart threats to national security, prevent or detect crime, and, ultimately prosecute offenders.

3.10.3 For example, taking communications data, during our inspections investigators have shared with us how they use the data to assist a victim to recall events – i.e. communications will often act as a prompt to put events into sequence. They describe how victims of bullying, harassment, nuisance & malicious communications, assault, sexual assault and attempted murder will often know the offender prior to being the victim of crime. They may have communicated with them on a regular basis - especially in the online environment. Within murder investigations the victim is, more often than not, found to have been in communication with their killer. The acquisition, collation and analysis of communications data within the boundary of an investigation or operation are a powerful tool.

3.10.4 There is an absence of consolidated guidance as to what may be done with the data outside the boundary of the justifications as to why the data was acquired in the first instance which we have broken down into simple issues –

- why, how and where is the data retained within the public authority;
- if the data is further processed beyond the reasons for its acquisition are the reasons recorded with a justification as to why;
- who may access it;
- what reviews are carried out to determine which data should be destroyed or further retained; and
- are each of these steps compliant with the Data Protection Act 1998.

3.10.5 There are further questions to be determined about what the arrangements are concerning the retention and processing of communications data relating to a victim or a witness and how their privacy is safeguarded.

3.10.6 This and other privacy safeguarding issues need to be properly considered by the heads of public authorities and those who advise them as, for example, police forces are now undertaking collaborations[21]. Those regions undertaking collaboration are sharing their capabilities and one can anticipate they will be developing processes and systems so as to bring enhanced services to their work which may include the collation of data lawfully acquired.

3.10.7 We say more about the audits that we undertake with regard to the use made of the intercepted material and communications data acquired in the next section of this paper. But it is this down-stream inspection of what was or what is, and just as importantly, what was not done with the material that makes, in our view, the IOCCO inspections unique in bringing more scrutiny to the process.

3.11 The case for prior judicial approval for interception and communications data

3.11.1 In recent months there have been many comments in the media concerning professions that handle privileged information (for example, lawyers and journalists). Comment has been made that the police should have obtained production orders authorised by judges (for example under section 9 of PACE) to obtain communications data in preference to the use of Chapter 2 of Part 1 of the Act. We launched an inquiry in early October this year in relation to the acquisition of communications data by police forces to identify journalistic sources as a result of the Interception Commissioner sharing the concerns raised about the protection of journalistic sources so as to enable a free press. Our inquiry is ongoing and we intend to report our findings early in the New Year.

[21] See Policing and Crime Act 2009 http://www.legislation.gov.uk/ukpga/2009/26/contents

3.11.2 In addition, a number of the leading organisations who defend privacy, free expression and digital rights have also put forward several principles to reform surveillance[22], one of which is "judicial not political authorisation". Many cite the practices elsewhere within the EU as being more conducive with the Convention requirements within Article 8.

3.11.3 Consequently we thought it would helpful to set out some additional information to assist in developing the debate relating to prior judicial approval for interception and communications data.

3.11.4 In 2011 the EU Commission undertook an evaluation of the Data Retention Directive (Directive 2006/24/EC) and reported their findings to the Council and European Parliament[23]. Several Member States supplied information as to what processes their law enforcement and intelligence agencies undertook to gain access to communications data. The submissions included who authorised access to communications data within their jurisdictions.

Table 1 - Access to communications data within the EU[24]

Member State	**Role of person authorising access**
Belgium	Authorised by magistrate or prosecutor
Bulgaria	Chair person of regional court
Czech Republic	*No submission made*
Denmark	Magistrate / judge
Germany	*No submission made*
Ireland	Garda Síochána - senior officer
Greece	Member of judiciary
Spain	Member of judiciary
France	Senior official in Ministry of Interior

[22] For example see https://www.dontspyonus.org.uk/org

[23] http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf

[24] See footnote 23 for source of Table 1

Italy	Public prosecutor
Cypress	Public prosecutor or judge
Latvia	Police investigators or public prosecutor
Hungary	Public prosecutor
Netherlands	Public prosecutor or investigating judge
Austria	*No submission made*
Poland	Police – senior officer
Slovakia	Public prosecutor or Police
Finland	No authorisation required for subscriber information. Judge's authority for traffic data
Sweden	*No submission made*

3.11.5 Many of the individuals cited above having a role as a public prosecutor or investigating judge may, to acquire access to communications data, grant an order for the *investigation* rather than for specific data (for example one order may authorise the acquisition of historic data and / or forward facing communications data for the investigation). These general orders might satisfy the basic necessity test, but we would question how proportionality can be judged properly under such a system. The exception to this practice appears to be limited to the United Kingdom, Ireland and France – those Member States have laws that require each acquisition of data to be considered and authorised individually. That is one of the reasons why the communications data statistics published by the EU Commission when reviewing the now defunct Data Retention Directive are misleading and not comparable – because in the UK an authorisation is necessary for each requirement of data.

3.11.6 It should also be noted that many of the Member States have a model that includes a public prosecutor who is directly involved in the "pre-trial investigation" and who may also authorise access to communications data within that investigation.

3.11.7 Prior approval of interception or acquisition of communications data would involve a judge assessing whether the case for necessity and proportionality has been made. This is obviously important, but perhaps of equal importance is to examine what was or was not done with the material after it was obtained or put another way, what conduct was undertaken and whether that conduct was foreseen by the person authorising.

3.11.8 An important element missing from the processes adopted within other jurisdictions is the absence of a formal review to reassess the proportionality of the conduct authorised and, if appropriate, the renewal or review of the warrant to intercept or the authority to acquire communications data. At the time of the application for a warrant relating to interception or the acquisition of communications data, the proportionality and collateral intrusion considerations are based at a particular point in time and, importantly, prior to any Article 8 interference being undertaken. In our view, in practice, an additional and appropriate test as to whether something is, was or continues to be proportionate to the Article 8 interference undertaken can only be obtained by scrutinising the operational conduct carried out, or put another way, the downstream use of the material acquired, for example examining –

- How the material has been used / analysed;
- Whether the material was used for the stated or intended purpose;
- What actual interference or intrusion resulted and was that proportionate to the aim set out in the original authorisation;
- Whether the conduct become disproportionate to what was foreseen at the point of authorisation and, importantly, question why the operational team did not initiate the withdrawal of the authority;
- The retention, storage and destruction arrangements for material acquired; and,
- Whether any errors / breaches resulted from the interference or intrusion.

3.11.9 This is what makes, in our view, the IOCCO inspections unique in bringing about scrutiny through audit within the operational environment where warranted interception and the acquisition of communications data is being used i.e. examining the Article 8 interference actually being undertaken. In a scientific sense, we test the operational hypothesis set down in the initial application that was authorised and though our observations might recommend its modification or require changes to operational practice to safeguard privacy. These are all important components when looking at the principles of necessity and proportionality and compliance with the legislation and it is crucial to examine those arrangements. If the UK moved to a prior judicial model similar to those used in the EU these key components would be lost.

3.11.10 It is also important to factor in the evidence gleaned from the prior judicial approval process that has been in place under the Protection of Freedoms Act 2012 for local authority access to communications data since November 2012. The Protection of Freedoms Act (2012) amended section 57 of RIPA to make clear that –

> *"it shall <u>not</u> be the function of the Interception of Communications Commissioner to keep under review the exercise by the relevant judicial authority…" [emphasis added]*

3.11.11 That amendment, in our view, put our inspections of local authorities on a less sound footing. We sought advice from the Home Office in relation to what action we might be able to take if we identified that, for example, a judge had inappropriately approved the acquisition of traffic data which a local authority is not permitted to obtain, or, approved a request where the necessity grounds under section 22(2) of the Act were not met; considering the fact that it is not part of the function of the Interception Commissioner to keep under review the judicial approval. This point still remains unclear.

3.11.12 We have previously reported our doubts that the introduction of a judicial approval process would lead to improved standards, or, have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data[25].

3.11.13 Only a handful of requests have been refused since November 2012 and the evidence that has been shared with IOCCO to date reinforces our view that the judicial approval process for local authorities has caused confusion, increased their operational costs (for example, in Scotland a £90.00 warranty application fee is charged by the Sheriff's Office to the local authority for each application) and produced no added benefit in seeking to better the scrutiny of applications. The level of scrutiny by the judiciary is also a concern - in one case the magistrate did not ask to see the application form which set out the necessity and proportionality justifications, or the DP's approval. The application was approved on the basis of a verbal synopsis from the applicant and the DP. It is extremely concerning that the paperwork was not examined in full to check that it had been properly authorised by the DP. In another case the magistrate approved the acquisition of traffic data which local authorities are not permitted to acquire, and in another, a request was refused and the local authority was directed to undertake what were arguably far more intrusive surveillance techniques prior to obtaining subscriber information (i.e. determining the name and address to a telephone). Many local authorities have provided reports of magistrates being unaware of the amendments to the Act and their new role, which is worrying particularly considering the Home Office gave a commitment to train magistrates to carry out this role properly.

3.11.14 Local authorities have also reported experiencing lengthy time delays in obtaining an appointment with a magistrate (for example, in the worst case 6 weeks). It is questionable after this period of time whether the necessity or proportionality justifications remain valid, notwithstanding the operational and evidence gathering opportunities that may have been lost in the intervening period.

[25] See Pages 63 and 64 of our 2012 Annual Report for more information.

3.11.15 In 2013 local authorities made 1766 of the 514,608 notices and authorisations for communications data (0.3%). There were also 2760 new interception warrants issued in 2013 in addition to numerous modifications and renewals which all required ministerial approval. Notwithstanding the logistical and cost implications of a prior judicial approval process being introduced, this section has also outlined other key points worthy of consideration –

- how to ensure proportionality is considered properly by maintaining individual authorisations;
- how to ensure there is down-stream scrutiny of the use, retention, storage and destruction of material and data;
- how to ensure a mechanism for the reporting of any errors or breaches; and,
- how to ensure adequate training.

3.11.16 Without consideration and inclusion of these key points a prior judicial approval process on its own would arguably provide fewer safeguards to protect privacy.

3.12 The case for an inspector-general or similar oversight model

3.12.1 The Act gives provision for four separate Commissioners' (the Interception Commissioner, the Intelligence Services Commissioner, the Chief Surveillance Commissioner and the Investigatory Powers Commissioner for Northern Ireland) and the Tribunal. In addition the Surveillance Camera Commissioner, the Biometrics Commissioner, the Intelligence Security Committee (ISC) and the Information Commissioner's Office (ICO) all have niche responsibilities relating to the oversight of surveillance powers.

3.12.2 There have been numerous debates on oversight reform in recent years. For example, the Justice and Security Bill green paper dated October 2011 set out a number of proposals, consultation questions, and, a possible model for an Inspector-

General[26]. The Justice and Security Act 2013 reformed the Intelligence Security Committee (ISC) and gave provision for the Prime Minister to direct the Intelligence Services Commissioner to keep under review any aspect of the functions of the Intelligence Services.

3.12.3 We understand how difficult it can be for individuals to understand the roles of the various bodies involved in overseeing the legislation concerning surveillance activity in the UK. We worked with the Information Commissioners Office (ICO) to assist them to produce the Surveillance Road Map[27] which provides an overview of who is responsible for what, and, the avenues open to individuals who wish to challenge any surveillance to which they are subjected.

3.12.4 The merging of the different RIPA Commissioners may simplify the oversight model from a public perception view. It may also assist with the consideration of the principle of proportionality – as at present for example, the Interception Commissioner looks at interception warrants and communications data applications in isolation and is not generally aware of any other activity under the Act that is authorised (for example, any directed or intrusive surveillance).

3.12.5 There may be a case for the various Commissioners' oversight to be linked to the conduct authorised and undertaken rather than being linked to a particular part of legislation as is the case now, which, in our view, can cause confusion as to who is responsible for overseeing what and when. By way of example, consider the following –

- Interception of communications -
    - the Interception Commissioner oversees and audits lawful interception of communications with a warrant[28]; whereas

[26] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228860/8194.pdf
[27] http://ico.org.uk/~/media/documents/library/Corporate/Practical_application/surveillance-road-map.pdf
[28] See sections 6 to 11 of the Act

- the Chief Surveillance Commissioner oversees and audits lawful interception without a warrant[29]; but
- no one oversees or audits the interception of stored communications when a statutory power or production order[30] is used to take possession or require it to be made available.

- Reporting of errors-
  - there is a requirement for errors to be reported to the Interception Commissioner relating to the acquisition and disclosure of communications data[31]; whereas
  - there is no requirement for errors to be reported by public authorities to the Interception Commissioner relating to conduct seeking to comply with a warrant for the interception of communications; but,
  - there is a requirement for errors to be reported by CSPs to the Information Commissioner relating to conduct seeking to comply with a warrant[32]; and
  - when CSPs report errors to the Information Commissioner[33] relating to conduct seeking to comply with a warrant they may be breaching a requirement within the United Kingdom to keep matters secret relating to warranted interception[34].

3.12.6 We maintain a working relationship with our colleagues in other oversight bodies to ensure there is no lapse in oversight or audit, but things could be more streamlined, made simpler. We believe these matters could be addressed by

[29] See conduct authorised within sections 3(1) and 3(2) of the Act

[30] See section 1(5)(c) of the Act

[31] See Chapter 6 of the Acquisition and Disclosure of Communications Data Code of Practice

[32] See **REGULATION (EC) No 1211/2009 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office –** and in particular *Article 2* - Amendments to Directive 2002/58/EC (Directive on privacy and electronic communications)-

- "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.'
- in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the **competent national authority**.

[33] Within the United Kingdom the Information Commissioner is the "competent national authority".

[34] See section 19 of the Act – offence for unauthorised disclosure

amending the various codes of practice accompanying the Act without a need to change the Act itself.

3.12.7 Merely merging the role of the Commissioners will not address this. The reality is that a merged oversight body would still require sub-teams of experts dealing with the conduct authorised by the various parts of the legislation which is, in effect, the position now. Furthermore in our 2013 Annual Report the Interception Commissioner commented that merged or enlarged oversight would risk bringing about a bureaucratic dilution of responsibility.

3.12.8 There is no doubt that one of the most important principles of oversight is independence – independence from Parliament and independence from Government. The Interception Commissioner is a former court of appeal judge and complete independence is the hallmark of any judge. The Interception Commissioner is not swayed by any political motivation and does not set out to or seek to defend, protect or promote the public authorities that his office is charged with overseeing.

3.12.9 Another important principle of oversight is to provide assurance to the public that the activities of the public authorities being overseen are reasonable, proportionate, necessary and compliant with all legal obligations, or to report where they are not. In a later section of this paper we outline the significant measures that we have taken in the last 18 months or so to improve transparency and provide further information about our work.

4. Transparency

4.1 Statistical requirements that should apply – communications data

4.1.1 Our annual report in 2012 and, again, in 2013, referred to the inadequacy of the statistical requirements in the Acquisition and Disclosure of Communications Data Code of Practice which accompanies Chapter 2 of Part 1 of the Act. The requirement is contained in Paragraph 6.5 of the Code of Practice, but essentially the public authorities are only required to report the number of authorisations and notices (written and oral) and the number of applications rejected.

4.1.2 The statistical information required by the Code of Practice is flawed for a number of reasons, including –

- more than 1 item of data may be requested on an authorisation or notice and therefore the number of individual items of communications data requested is not reported. This figure will be higher than the number of authorisations and notices;
- the different systems in use by public authorities have different counting mechanisms for notices and authorisations. For example, one public authority may request data in relation to 3 telephone numbers on 1 notice, whereas another public authority may request the same 3 items of data on 3 separate notices. The result would be an over inflated number of authorisations and notices for the second public authority. This makes meaningful comparisons difficult; and
- it is a requirement for public authorities to report the number of applications that have been *rejected* each calendar year, but not the number of applications that were approved. Therefore it is difficult to establish accurately the percentage of applications rejected.

4.1.3 Following interest on Twitter we recently published a guide to explain the relationship between applications, authorisations, notices and items of data on our

website.[35] We have consulted with the Home Office and set out the revisions and enhancements of the statistical requirements that we believe are necessary both to assist us with our audit role, and, to better inform the public about the use which public authorities make of communications data.

4.1.4 During the debates concerning the Data Retention and Investigatory Powers Bill the Minister James Brokenshire stated the Government will be amending the code of practice on the acquisition and disclosure of communications data later this year (see Hansard 15 July 2014: Column 816)[36]. We have urged the Home Office to expedite matters to bring about early public consultation. Our statistical requirements are published in Annex A of this paper for the review to consider.

4.1.5 In our 2013 Annual Report we outlined that a number of CSPs are releasing transparency figures in relation to the communications data disclosures they make to public authorities. Although it is laudable that these CSPs are trying to improve transparency and better inform their customers about how they respect their privacy, their statistics should be treated with extreme caution as again different counting mechanisms and rules are applied which can result in misleading comparisons. In our view the statistical information should be collected by the public authorities, under required conventions and counting mechanisms to ensure that it is comparable and accurate.

4.2 Statistical requirements that should apply – interception

4.2.1 There are no statistical requirements in the interception of communications data Code of Practice. The section 19 secrecy provisions make this area challenging.

4.2.2 To date we have only reported the overall number of new warrants issued and the number of extant warrants at the end of the calendar year. It may be

[35] http://www.iocco-uk.info/docs/Relationship%20between%20applications,%20authorisations,%20notices%20and%20items%20of%20data.pdf

[36] http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140715/debtext/140715-0004.htm

possible to breakdown the total number of warrants by statutory necessity purpose (i.e. national security, serious crime, economic well-being of the UK) without prejudicing national security, and, we believe this statistic would better inform the public as to the use of these powers. A view could be taken that it would be damaging to national security to go further that this, for example, by breaking down the number of interception warrants by agency. But of equal value is the consideration as to whether the publication of further statistics on their own actually brings about better transparency.

4.3 Transparency - public authorities

4.3.1 We have encouraged the public authorities who make use of powers under the Act to engage with and contribute to the various reviews, including this one. It is also important for the public authorities to contribute to the Code of Practice consultations. This will help to ensure the various reviews and debates are informed and evidence based.

4.3.2 The public authorities also need to think about how they can better inform Parliament and the public about why they need their powers, how they make use of their powers, and, why any additional capabilities might be required.

4.4 Transparency - Oversight bodies

4.4.1 This paper has already outlined that one of the most important principles of oversight is to provide assurance to the public. We have taken significant steps in the last 18 months or so to improve transparency and provide further information about our work including –

- Annual Report - We published more detail than ever before in our 2013 Report and recommended to the Prime Minister that there should be no confidential annex;

- Website – We publish regular press releases and information in relation to the scope (and findings) of inquiries we are undertaking, responses to legislative changes, presentations or speaking notes from events attended; detailed documents explaining more about areas of our work etc;
- Twitter feed – We tweet about our inquiries and publications and re-tweet items of interest or relevance to our work;
- Public Events – We have given written and / or oral evidence to several parliamentary select committee inquiries, the Intelligence Security Committee, various reviews of powers and Government consultations. We also regularly give speeches; and attend roundtables and panel discussions at various Government, civil society, legal and industry events.

4.4.2 We intend to continue to push the boundaries in relation to how open and transparent we can be about our work to improve public confidence and understanding and contribute to ensuring any debates are informed.

5. Summary of points for the review to consider

We have already cited the background to these points in detail within the main body of this report.

5.1 Safeguards to protect privacy

The right to effective remedy

- The current threshold of "*wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers"* appears artificial as the Act creates no such threshold to engage the Investigatory Powers Tribunal ("the Tribunal). What threshold should apply as wilful or reckless appears too high?

- At what point should a citizen be advised to engage with the Tribunal?

- Article 13 of the ECHR is absent from the Human Rights Act 1998. Whilst citizens may, in normal circumstances, be able to seek a remedy by pursuing an action through the civil or criminal courts they can only do that when in possession of certain facts. If the law prohibits certain facts being made known to them they will, in reality, rarely be in possession of sufficient information to formulate the basis of a complaint - what is the effect if a citizen is unable to gain access to effective remedy?

- Should the Act be amended to enable the Interception Commissioner to make a complaint to the Tribunal on behalf of a citizen who, in our opinion, has had their rights interfered with in a manner contravening law?

- Should the Tribunal be able to deal with complaints relating to a wrongful act by a CSP when responding to a lawful requirement by a public authority – for example, when the CSP intercepts communications or discloses communications data in error?

The definition of content and communications data

- Does the determination of what constitutes the content of a communication within the online environment require better defining within the Act?
- Does the definition of subscriber information need refining or reviewing now that it potentially covers a wider catchment of data than originally available?

Authorised access to communications data

- Does the review consider the rank / level of the prescribed Designated Persons (DPs) within public authorities to be sufficient, particularly when taking into account the detail that is now captured by the term subscriber information?
- Does the review consider that the prescribed DPs are comparable across the different public authorities?

Interception error reporting provisions

- Does the review consider that there should be an equivalent error provision in the Interception of Communications Code of Practice to that in the Communications Data Code of Practice?

The role of the Single Point of Contact (SPoC)

- Does the review consider that the role of the SPoC needs to be defined in the Act, amplified in a revised Code of Practice, and, further enhanced by the publication of professional minimum competencies by the Home Office and College of Policing?

Requirements for CSPs to retain communications data

- Does the review consider that Parliament should amend the DRIPA or the Act to include a provision that requires the Interception Commissioner to oversee, audit and report on the necessity and proportionality of notices given by Secretary of State requiring the retention of specific communications data by a CSP; and whether DRIPA widens the retention

requirements when compared to the Data Retention (EC Directive) Regulations 2009 which it replaced?

Non-compliance by CSPs in relation to requirements to intercept communications or disclose data

- Should Parliament amend the DRIPA or the Act to include a provision that requires the Interception Commissioner to oversee, audit and report on instances when CSPs, within the United Kingdom or elsewhere, fail or refuse to intercept communications or disclose communications data when a lawful requirement is made of them within the Act?

Use of other powers to acquire communications data

- Should Parliament amend the Act so as to require the Interception Commissioner to oversee, audit and report to the Prime Minster on the use of other laws to acquire communications data?
- Should Parliament go further and amend the Act to include a provision that stops the use of other laws to acquire any form of communications data?

Use of other powers to acquire the content of stored communications

- Should Parliament amend the Act to include a provision that requires the Interception Commissioner to oversee, audit and report to the Prime Minster on the use of other powers to acquire the content of stored communications (for example, the use of section 9 PACE Orders).

Use, retention, storage and destruction of the communications data acquired

- Should IOCCOs audits be extended to include the oversight of the retention, storage, processing, and destruction of communications data that have been acquired by public authorities?

- Does the review consider that there needs to be consolidated and / or additional guidance within the Code of Practice concerning the retention and / or further processing of communications data beyond the justifications / reasons for its acquisition using Chapter 2 of Part 1 of the Act?

The case for prior judicial approval for interception and communications data

- If the UK were to move to a prior judicial approval process;
  - Should an authorisation be required for each single data or interception requirement, or, a general authorisation be provided for an investigation?
  - How would the member of judiciary review and / or renew the authority to continue interception or the acquisition of communications data?
  - How would the use, retention, storage and destruction arrangements be scrutinised?
  - Should there be a mechanism for the reporting of any errors or breaches?

5.2 Transparency

Statistical requirements that should apply – communications data

- Does the review consider the suggested enhancements to the communications data statistics at Annex A are sufficient to meet the statistical and transparency requirements envisaged?

Statistical requirements that should apply – interception

- The section 19 secrecy provisions make this area challenging – does the review consider there is provision within the Act that we can utilise more effectively to better inform the public as to what has been done in matters relating to interception?

Transparency – public authorities

- Should public authorities do more to inform Parliament and the public about why they need their powers, how they make use of their powers, and, why any additional capabilities might be required?

Transparency – oversight bodies

- What other avenues might we (and other oversight bodies) adopt to expand our audit, probe areas of concern, bring about more transparency, and, better inform the public?

Annex A
Enhanced Statistical Requirements under Chapter 2 of Part I of RIPA

The suggested statistical requirements for the revised Code of Practice will include:

- The number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data;
- The number of applications submitted by an applicant to a SPoC requesting the acquisition of communications data, which were referred back to the applicant by the SPoC for amendment, including the reason for doing so;
- The number of applications submitted to a designated person for a decision to obtain communications data, which were approved after due consideration;
- The number of applications submitted to a designated person for a decision to obtain communications data, which were rejected after due consideration, including the reason for rejection;
- The number of notices requiring disclosure of communications data;
- The number of authorisations for conduct to acquire communications data;
- The number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;
- The number of **items of communications data** sought, for each notice given, or authorisation granted[37].

Then, for each **item of communications data** included within a notice or authorisation the public authority must also keep a record of the following:

- The Unique Reference Number (URN) allocated to the application, notice and/or authorisation;
- The statutory purpose for which the item of communications data is being requested, as set out at section 22 (2) of RIPA;

[37] One item of communications data is a single communications address or other descriptor included in a notice or authorisation. For example, one communications address that relates to 30 days of incoming and outgoing call data is one item of communications data.

- Where the item of communications data is being requested for the purpose of preventing or detecting crime or of preventing disorder, as set out at section 22 (2) (b) of RIPA, the crime type being investigated;
- Whether the item of communications data is traffic data, service use information, or subscriber information, as described at section 21 (4);
- A description of the type of each item of communications data included in the notice or authorisation[38];
- Whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- Whether the data relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, Member of Parliament, or Minister of religion);
- The age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;
- Where an item of data is service use information or traffic data retained by the CSP, an indication of the total number of days of data being sought by means of notice or authorisation;
- In the case of items of service use information or traffic data sought by means of a forward facing notice or authorisation, this will relate to the number of days of data disclosed or acquired[39];
- The CSP from whom the data is being acquired, including whether this service provider is based in the United Kingdom or elsewhere;
- The priority grading of the item of communications data;
- Whether the item of communications data is being sought by means of the urgent oral process.

December 2014

[38] The data type is to include whether the data is telephone data, whether fixed line or mobile, or Internet data. Guidance on specific data types to be collected may be issued by, or sought from, IOCCO.

[39] In the case of a forward facing notice or authorisation, the number of days of data sought will often differ from the number of days of data disclosed or acquired. This is because a forward facing notice or authorisation will often be withdrawn or cancelled at the point it has served its purpose. For example, if the purpose is to identify an anticipated communication between two suspects, the notice or authorisation may be withdrawn subsequent to that communication being made.

ISPA

About ISPA

The Internet Services Providers' Association (ISPA) is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and actively represents and promotes the interests of businesses involved in all aspects of the UK Internet industry.

ISPA membership includes small, medium and large Internet service providers (ISPs), cable companies, web design and hosting companies and a variety of other organisations that provide internet services. ISPA currently has over 200 members, representing more than 95% of the UK Internet access market by volume. SPA was a founding member of Euro SPA.

We have been involved in the area of communications data for many years, including the passing of the Regulation of Investigatory Powers Act (RIPA), the development of data retention provisions under both the Anti-Terrorism Crime and Security Act (2001) and the Data Retention (EC Directive) Regulations 2009. Most recently we responded to the Joint Committee on the Draft Communications Data Bill and the Data Retention and Investigatory Powers Act. A number of our members are subject to obligations under RIPA and associated legislation.

Introduction

ISPA welcomes the opportunity to respond to the Review of Communications Data and Interception Powers (the Review).

The Review is much needed, not only because the leaked information provided by Edward Snowdon has fundamentally changed public understanding and scrutiny of surveillance issues, but also because of the significant increase in the use of internet communications since the passing of RIPA. What was once a policy issue that received only limited amount of specialist attention, the access to and use of communications data is now a major political issue and one that deserves sufficient time and resources for scrutiny.

ISPA's members accept that law enforcement agencies should have reasonable lawful access to communications data in order to help in the detection and investigation of serious crime and to safeguard national security. However, SPA members also share concerns raised about the UK data retention regime and recent reform efforts.

Some of the elements of the current regime perform well and should be retained in any future reform programme. For example, the Single Point of Contact System (SPOC) has provided for effective means of structuring the relationship between law enforcement (LEAs) and ISPs. The current system also provides for the recovery of the costs that CSPs incur when they comply with requests. It is important that this continues so that CSPs' continued investment in innovation and service development is not adversely impacted by data retention requirements. Cost recovery further acts as an important safeguard as it ensures that law enforcement only requests data where the cost can be justified .It is crucial that these elements continue as part of any future communications data regime. In the remainder of this document, we set out our thoughts on the policy making process in the area of communications data and what we hope the Review will achieve. We further outline a number of principles that should govern any future reform efforts.

Summary of main points

- Since the passing of RIPA in 1999, there has been insufficient consultation with industry and other stakeholders
- Government has failed to facilitate an open debate around communications data and interception and amendments have been made without meaningful scrutiny
- The Review is a first and vital step in ensuring that policy is developed in line with proper process and standards of consultation
- The CJEU's judgment on the Data Retention Directive highlighted the need for data retention regimes to be structured in a way that complies with the principle of proportionality and fairly balances the requirements of law enforcement, privacy of users and the impact on business
- We suggest five principles that should guide policy development in this area:

1. Data minimization - Data retention should be limited as far as possible both in terms of data being retained and accessed
2. Oversight maximization - Data retention should be governed by a clear legal framework in which executive powers are subject to strong checks and balances
3. Transparent operation - Data retention risks undermining public trust in communication networks if government does not publish information about the number of requests made to ISPs
4. Jurisdictional respect - Any data retention regime must allow for a clear, robust and workable system to govern cooperation across jurisdictions
5. Competitiveness - The impact of a communications data regime must protect the UK's position as an attractive arena for digital businesses

An area that we do not cover in detail in the remainder of the response but that is nevertheless important to us is how Part 1, Chapter 1of RIPA applies to and affects the day-to-day operation of providers. RIPA was essentially drafted for the world of postal and telephone communications and its provisions make it very difficult to determine whether activities carried out by a provider constitute lawful or unlawful interception. This is particularly relevant in a time where providers are being asked to play a greater role in the protection of their customers, e.g. in relation to the provision of network level parental control solutions or malware protection. This issue should be kept in mind in any reform of RIPA and guidance for ISPs is essential.

Thoughts on the policy making process and what we hope the Review will achieve

The Government's decision to undertake an independent review of the use and governance of communications data and interception in the UK is a marked and welcome change from previous experience. There has been little comprehensive consultation with industry (and we understand other stakeholders) to fully evaluate and review communications data and interceptions powers since the passing of RIPA in 1999. The debate around communications data and interception is also complex and that concerns about security and confidentiality sometimes limit what can be revealed publicly. However, Government should have done more to ensure that policy is developed in an open and transparent manner.

The requirements of law enforcement, privacy of users and the impact on business can only be properly balanced if policy development and political debate are based on a sound evidence base and sufficient time is provided to those who have to make the final decision and those who wish to influence the process. This requires that the Government is open and forthcoming about its aims and stakeholders are given the chance to provide input during both the pre-legislative process and when legislation is discussed in Parliament. Recent debates around communications data demonstrate that this has not always been the case, e.g. in relation to the passing of the Data Retention and Regulatory Powers Act 2014 (DRIPA) and the proposals for a Communications Data Bill.

The Government has insisted that the recently passed DRIPA does not provide for an extension of current powers to intercept and use communications data even though it can be argued that DRIPA allows the new application of RIPA powers to communications services and entities both within and outside the UK that were not clearly covered by the previous legislation. By framing the debate in such a way and by relying on an accelerated parliamentary process, the Government has effectively created a situation where Parliament has passed a new Act without being able to have a thorough and informed debate.

While the Joint Committee on the Draft Communications Data Bill extensively consulted with stakeholders, it is still the case there was only limited meaningful consultation as Government did not allow for any structured input during the actual drafting process. This was recognised by the Committee which concluded that more consultation with industry, technical experts and others was needed and that meaningful consultation can take place only when there is "clarity as to the real aims of the Home Office."[1] Even though the Joint Committee's very clear conclusion was accepted by the Home Office, there have been no further attempts to properly consult with industry, even with the introduction of DRIPA which, in the eyes of some observers, significantly extends capabilities in certain areas. Government may argue that it does meet with stakeholders but we contend that it is not conducted in a properly open and comprehensive way.

We see the Review as a first and vital step in ensuring that policy is developed in line with proper processes and standards of consultation. Given the complexity of RIPA and the Government's approach to consultation, it is no surprise that the policy process has at times failed to fully engage with the intricacies and implications of some of the reform proposals that have been made in recent years. Going forward, Government needs to foster a full and informed debate by:

- Developing policy within an open and transparent framework
- Allowing time to debate complex issues fully with all stakeholders, including industry and civil society and user and human rights groups
- Being clear about the scope and aims of reform proposals

Five principles for achieving a better communications data regime

In its recent judgement, the Court of Justice of the European (CJEU) declared the European Data Retention Directive invalid. Whilst the judgement does not directly apply to the UK data retention regime we believe that it provides a useful starting point for considering a number

[1] Joint Committee on the Draft Communications Data Bill (2012), Draft Communications Data Bill, p.75

of principles which should govern any future reform efforts.

The CJEU found that by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data. The Court also found that the fact that data are retained and subsequently used without the subscriber or registered user being informed, it is likely to generate a feeling that their private lives are the subject of constant surveillance.

While the Court accepted that the Directive satisfies an objective of general interest (namely the fight against serious crime and, ultimately, public security) it ultimately failed to comply with the principle of proportionality by failing to ensure that the interference with fundamental rights (e.g. right to private life and to the protection of personal data). The Court touched on a number of issues and the following are of particular importance:

- Coverage, in a generalized manner, of all individuals, all means of electronic communication and all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.
- Failure to lay down any objective criterion which would ensure that the competent national authorities have access to the data and instead simply refers in a general manner to 'serious crime' and does not require any prior review by a court or by an independent administrative body.
- Lack of objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

It is not for ISPA to undertake an in-depth legal assessment of the UK data retention regime on the basis of the OEU judgement. However, the key issue going forward will be to ensure that the UK data retention regime takes account of the judgment and is proportionate and fairly balances the requirements of law enforcement, privacy of users and the impact on business. The following principles should guide policy development:

1. Data minimisation - Data retention should be limited as far as possible both in terms of data being retained and accessed
2. Oversight maximisation - Data retention should be governed by a clear legal framework in which executive powers are subject to strong checks and balances
3. Transparent operation - Data retention risks undermining public trust in communication networks if government does not publish information about the number of requests made to CSPs
4. Jurisdictional respect - Any data retention regime must allow for a clear, robust and workable system to govern cooperation across jurisdictions.
5. Competitiveness - The impact of a communications data regime must protect the UK's position as an attractive arena for digital businesses

Data minimisation

While it may not be possible for law enforcement purposes to disclose exact details of who and what is being subjected to data retention, the current data retention regime in the UK allows for the blanket collection of communications data for virtually any communications service and risks undermining public trust in modern communications media. The use of broadly defined reasons to justify the access to data, e.g. "preventing or detecting serious crime" also does not provide sufficient safeguards to ensure that the private data is being used in entirely appropriate ways. With this in mind, we believe that the data retention regime should codify sensible limitations on Government's ability to compel service providers

to retain and disclose data. Limits should apply in relation to:

- the types of data subject to retention;
- the individuals subject to retention; and the
- purposes for which the data can be disclosed and accessed.

We would particularly welcome if the Review explored more targeted means of capturing and accessing communications data. For instance, the viability of relying on data preservation rather than retention as a means to limit the number of individuals that are directly affected by data retention. Additionally, clear legal barriers should be inserted in the acquisition process for communications data to ensure that data is not provided without a full assessment and balancing of competing rights. This is particularly relevant for cases where RIPA can be used to acquire information about whistle-blowers, sources of journalists or conversations between doctors/journalists and their clients. It reaffirms the need to clarify the definitions of serious crime and national security that RIPA was originally intended for and the need to impose clear limitations on where RIPA should not be used.

Oversight maximization

Communication is more data driven than ever yet the UK still relies on a data retention regime that was essentially drafted to regulate the retention and use of communications data for telephony and email communication. The privacy impact of communications data generated by modern communication services, such as social networking, can be more revealing than the more traditional services. It is therefore crucial to consider the ability of law enforcement and other competent authorities to combine data sets from different communication services which again may have a more severe privacy impact. As such it is vital that oversight mechanisms are able to keep up with technological developments. With this in mind, we believe that any data retention regime should be governed by a clear legal framework in which executive powers are subject to strong checks and balances. This implies that:

- Parliament needs to be enabled to have an informed debate and make an informed choice before and after relevant regulations are passed;
- Mechanisms for the day to day oversight are well resourced fully independent and effective; and
- Mechanisms are provided to clarify the law where powers are not clear or disputed.

We would particularly welcome if the Review investigated how the existing oversight mechanisms can be strengthened and improved. Aside from providing more resources and recruiting Commissioners from a more diverse set of candidates, the remit of the oversight bodies could be expanded. Instead of merely spot checking whether the proper processes for the retention and acquisition of communications are adhered to, Commissioners could seek to undertake a more in- depth assessment of whether powers are used correctly and whether the rights of users are properly balanced with the interests of law enforcement. This would be particularly relevant if Government decided to extend its capabilities in line with the proposals for the Communications Data Bill. To assist with this, Commissioners should utilise expertise from industry, law enforcement, user groups and human rights representatives to challenge and inform working practices and processes, e.g. through a formal advisory board. There may also be merit, either within or outside the existing oversight bodies, in allowing users and

providers to clarify the law where powers are not clear or disputed, e.g. if existing powers are applied to a new service that may allow access to data with greater privacy impact.

Transparent operation

Transparency is crucial for maintaining public trust in modern communication networks and underpins the whole debate around data retention. Oversight mechanisms are strengthened if their findings are publicly available and can be subjected to an independent assessment. Public trust can be maintained if meaningful information is provided about the scale of data retention. This implies that:

- Government should allow oversight mechanism to publish detailed information about the number and nature of government demands for user information and about the day-to-day operation of the communications data regime
- Government should allow private companies to publish the number and nature of government demands for user information if they wish to do so.

Jurisdictional respect

The global nature of Internet services means that international cooperation is vital. Any data retention regime must allow for a clear, robust and workable system to govern legal requests across jurisdictions and protect existing good cross-border relations. In doing so, the regime must:

- Respect existing jurisdictional arrangements and international law and where necessary review improve existing arrangements, e.g. MLATs in the first instance
- Require Governments to work together to address issues with access to data with the goal of providing clear legal frameworks which provide certainty for providers
- Provide mechanisms for ensuring requests from LEAs are proportionate and necessary, and not overly broad or framed in a way that would circumvent the laws of the UK or other countries.

Competitiveness

The impact of a communications data regime must protect the UK's position as an attractive arena for investment, development and growth of digital businesses - one of the most important sectors to the UK economy. The Internet sector is constantly innovating to offer customers new ways of communicating and consuming or producing content, often led by start-ups. There is a real danger that these services and providers could be subject to communications data retention requirements, fundamentally changing how these (often small) businesses operate. There is also a danger that due to jurisdictional issues, UK providers are asked to retain data of overseas third party services that is transmitted over their network which would further disadvantage them in the market place.

To limit damage to competitiveness and innovation the regime must:

- Provide clarity over what data is in scope and empower Parliament and independent oversight bodies to help define this data;
- Include comprehensive and transparent impact and cost assessments; and
- Minimise the possible damage to CSPs and the UK as a place to do business.

It is worth adding that due to the extra-territorial application of the UK regime, other countries, including those with more authoritarian regimes, may feel entitled to not only enact similar data retention powers but also apply to them to operators purely operating in

the UK. The review should factor in that UK policy in this area is developed and replicated elsewhere.

Conclusion

The Internet is fundamental to how we live our lives; not only is it a primary means of communication, it underpins the economy and is a real engine for growth and change. It is vital that policy decisions made in the area of communications data and interception do not undermine trust and security in modern communications networks. The UK must adopt a regulatory framework that works for law enforcement, users and industry and we have set out five principles to guide the reform process.

The Review is a first step in ensuring that the wider policy is developed in line with proper process and standards of consultation. However, we are concerned that the debate around communications data could once again become politicised and urge all political parties to take account of the independent Review's findings instead of falling back on already established policy positions. Achieving a regime that manages to proportionately balance competing interests is a challenge but getting it right will help the digital economy to continue to thrive and innovate whilst maintaining the ability to investigate serious instances of crime.

October 2014

Internet Telephony Services Providers' Association

Response to the Joint Committee on the Draft Communications Data Bill

About ITSPA

The Internet Telephony Services Providers' Association (ITSPA) is the UK VoIP industry's trade body, representing over 60 UK businesses involved with the supply of VoIP and Unified Communication services to industry and residential customers within the UK. ITSPA pays close attention to the development of VoIP and IP regulatory frameworks on a worldwide basis in order to ensure that the UK internet telephony industry is as competitive as it can be within international markets.

Please note that certain aspects of the ITSPA response may not necessarily be supported by all ITSPA members. Individual members may respond separately to this call for written evidence where a position differs.

A full list of ITSPA members can be found at http://www.itspa.org.uk/

As the joint committee will understand, it is difficult for a trade association with a broad membership to respond to each individual question with a uniform answer. Members have different experiences surrounding data requests from law enforcement and local authorities and different positions (based on the services they supply) on the proposed legislation put forward by the Coalition Government. We have responded in general terms, following several discussions with our members and highlighted specific points of concern and interest which we hope the Joint Committee can investigate further. ITSPA members would welcome the opportunity to discuss specific points at greater length with the Joint Committee, should it be deemed necessary.

General Comments

ITSPA welcomes the opportunity to provide written evidence to the Joint Committee on the Draft Communications Data Bill. It is an important piece of legislation that needs to be scrutinised effectively to ensure a workable process can be implemented. Law enforcement organisations must have access to the communications data they need to tackle serious crime, however the communications industry must not be overburdened with a regime that causes operational difficulties or infringes on their customers privacy. Whilst ITSPA

accepts the sensitive nature of some of the issues surrounding this legislation, the confidential nature of some areas have made it difficult for our members to respond as comprehensively as we would like. We would urge the Joint Committee to gain greater detail from the Home Office in order to provide industry with greater clarity of the long term implications of the draft Bill.

The main concerns for ITSPA members in terms of scope are the precise type of data sets that will be required in the future and the exact requirements surrounding both third party data and compliance of overseas providers. These are key areas that we believe the Joint Committee should focus on to ensure the proposals can work in practice.

Law Enforcement Requirements

As previously mentioned, ITSPA recognises the importance of communication data for law enforcement agencies as they seek to prosecute crime. We accept that the way people (and criminals) communicate is shifting, due to changes in technology. It is important that law enforcement keeps up with these trends. ITSPA members cooperate fully with the data requests under the existing legal framework.

From an initial perspective, particularly for 'pure' VoIP providers (those providing only IP telephony and not other services like instant messaging), there would appear to be only minimal changes to the current obligations. However we do have concerns surrounding any future requirements that this Bill may bring on the VoIP industry, which is not clear in either the content of the draft Bill or in discussions with the Home Office. There appears to be a lack of clarity as to whether other data sets (not retained for normal business purposes) will have to be retained by telecommunication providers in the future and it is therefore hard for ITSPA to make an assessment of the long term implications for the industry. We accept our responsibilities to support law enforcement agencies but the relationship must be built on trust and effective communication as to how this legislation may affect the industry going forward.

We would also question the suggestion that this draft legislation is merely maintaining current capabilities for law enforcement agencies. Whilst it is true that the draft Bill is focussed on bringing new technologies into the scope of the current regime, there are a number of other areas that strongly suggest an extension of scope. These would include the new filtering arrangements, retention of third party data and the changing of definitions surrounding communications data and telecommunications providers. This does not necessarily impact the majority of our members (at least in the short/medium term but it will have an impact to the wider communications industry and could potentially impact VoIP providers in the future. This is why ITSPA requests further clarity on the proposals and we would ask the Joint Committee to investigate further.

Filtering Arrangements and Technical Issues

There are also significant concerns as to how a filtering system would work without significantly disrupting communication providers' (CPs) operations, inadvertently capturing communications content, and/or creating dangerous opportunities for the leakage of sensitive data or data fraud.

ITSPA would welcome further investigation into how data will be collected under a notice and how the filter will interact with the CP. There have been suggestions that the Home Office may require a direct feed to the providers' data base. This could cause a number of problems in terms of both consumer data security and for the operations of a CP. There are also questions marks surrounding how the interaction with the filter will be affected by any network upgrades or configuration changes that the CP may need to undertake. This could cause both operational problems and have financial implications for the CP; it is unclear as to whether this element of cost recovery would form part of the Home Office's new obligations. Equally there are competition concerns around this point. CPs who have not received a notice and do no interact with the filter, will not be hampered by the potential hazards surrounding network upgrades. Further information on how the filter would work is vitally important. ITSPA members would be concerned if a similar system to the Netherlands were adopted, whereby CIOT(the authority responsible) can require that registered communications providers install a direct feed into their servers so that CIOT can download data every 24 hours. We believe that the Dutch arrangement is not proportional to the need and can result in serious implementation issues for CPs.

In terms of some of the technical queries outlined, ITSPA does believe that there are vendors who are able to offer the solutions to capture the necessary communications data. However, the safety and security concerns cannot be underestimated. It would be an extremely challenging process for the industry to undertake. CPs would be obligated to ensure third party data was captured and that the filter could cope with enormous volumes of data. Such data, when aggregated, becomes important and extremely sensitive information, which increases the business impact and security threat. Some data may include government data up to the Restricted level (as is allowed over the ISDN). The costs of storing such data can be prohibitive and the risks must be evaluated properly.

Costs

ITSPA does not believe that the Government estimate of £1.8bn over 10 years is realistic. We feel there are too many factors that may contribute to this cost rising significantly. It could cost large CPs hundreds of millions of pounds to integrate and store data correctly, to include third party data and other information that they would not usually store for business purposes. Over time, as data requests are made to smaller providers, the extra costs will also filter down, creating a significant financial burden.

There is also an assumption by the Home Office that access to data from overseas providers will be relatively straight forward. ITSPA members are less convinced this will be the case and we believe that costs could be higher than estimated. Future developments and capabilities within the communications space will also mean that law enforcement agencies may have to shift their focus to other methods of communication and this will inevitably mean a stark increase in overall costs.

We welcome the Home Office's commitment to cost recovery and would stress this as a requirement for any final legislation. This commitment is fundamental to ensure an effective system is maintained. Whilst ITSPA has not had insight into how the Home Office has costed their proposals, we fear figures are too optimistic, given the technical challenges that the wider communications industry may experience.

In terms of costs benefits, the ITSPA does accept that there could be considerable savings and suggest that this could even exceed the £5-6bn suggested. The more effective the communications data that law enforcement receive, the more efficient they will become at solving crimes, catching criminals and coping with major incidents (such as public disorder). This will create financial efficiencies within the respective organizations and reduce the financial loss that both individuals and organizations experience when they are victims of crime and fraudulent activity. However, as previously indicated, IPSPA does expect the costs to implement these changes to be more expensive than predicted which needs to be taken into consideration when deciding the true value of the draft Bill for both law enforcement organizations and society as a whole. Given the economic constraints on Government at present, there is a need to ensure the financial costs are truly going to bring tangible benefits.

Safeguards and Oversight

The filter will have access to an enormous amount of data and will need some strong controls to prevent misuse and protect against criminal hacking. There is also the concern that it will be unavoidable in some instances to prevent collating content. Certain information required by enforcement agencies will contain content embedded in the data that cannot be removed without destroying the data. For example, in web access logs the destination urls can contain information that discloses the nature of the content.

ITSPA feel that in terms of the existing communications data that is stored or for data that is anonymous, the safeguards currently in place would be sufficient. However a warrant system should be considered for data that included content when it was not possible to supply anonymous access data without rendering the data meaningless.

In terms of everyday oversight, ITSPA members are generally happy with responsibility being devolved to the Interception of Communications Commissioner's Office (IoCCO) and the Information Commissioner's Office, provided they are sufficiently resourced and have the technological understanding of the services being used. There have been questions raised by some members surrounding the amount of parliamentary oversight to the draft Bill and whether too much power will lie with the Home Secretary in this area once legislation is passed.

ITSPA members are satisfied that the sanctions currently in place under the present regime will be sufficient under any revised legislative framework.

August 2012

The Law Society

Introduction

The Law Society of England and Wales is the professional body representing more than 145,000 solicitors in England and Wales. It works globally to support and represent its members, promoting the highest professional standards and the rule of law.

1. Overview

We are grateful for the opportunity to provide evidence to the first stage of the current review of communications data and interception powers in the UK. Such a review is long overdue and it is regrettable that the price of holding it was the passage of the Data Retention and Investigatory Powers Act 2014 (DRIPA), which also mandated it.

We hope that the review marks the start of a journey that will end with Parliament simplifying and clarifying a complex and confusing legal framework. Surveillance law should strike a better balance between security and privacy – one that is better understood and one that commands greater public assent.

We have grouped our comments around the scope of the review as set out in DRIPA s.7(2) and in the published terms of reference.

We would however like to make some general opening observations.

- The ability to mine communications data is now so great that much information about individuals' activities and lives can be gleaned simply from their traffic; and consequently the distinction between data and content is no longer so important in the determination of legislative interference and safeguards;

- The legislation is in a mess and contradictory - the fact that it is neither accessible nor intelligible is an affront to the rule of law and the requirement in ECHR Art 8(2) that interference be "in accordance with the law" - as to which see Halford and Malone. The law has not kept pace with technological developments and needs overhaul.

- We need to develop a coherent set of principles to determine what should be the limits of permitted surveillance and how such surveillance should be policed.

2. Current and future threats and the capabilities to combat them

The public have been given differing accounts of the surveillance capabilities of the UK government. On the one hand, the Snowden revelations suggest that GCHQ and

its allies have exceptional technical intercept capability; on the other, the Home Office argues that there is a 'capability gap'.

According to reports based on documents provided by Snowden, GCHQ and the NSA have exceptional technical capabilities.

In June 2013, the Guardian reported that GCHQ personnel had attached intercept probes to the transatlantic fibre-optic cables running into Europe through Britain. These cables carry data including data generated by phone calls, email messages, social media and web browsing. According to the article 'For the 2 billion users of the world wide web, Tempora represents a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world'.

There have also been allegations that GCHQ acted illegally by accessing communications content via the NSA's PRISM programme (a programme through which the US Government obtains intelligence material from Internet Service Providers (ISPs)). Parliament's Intelligence and Security Committee (ISC) concluded that GCHQ had not circumvented or attempted to circumvent UK law, but this is further evidence of capability.

The ISC has accepted Home Office assertions of a so-called a 'capability gap'. This is the gap between what communications data the agencies need access to and what communications service providers (CSPs) currently retain for "internal business reasons" (*Access to communications data by the intelligence and security Agencies*, February 2013). Data are lost between service infrastructure providers like BT and application service providers like Facebook; single communications are fragmented between numerous service providers and overseas CSPs "cannot be obliged to provide [relevant data] to … UK authorities'.

The ISC concluded that the shortfall between the data required by the Agencies and that which the CSPs – both domestic and overseas – hold for their internal business reasons is significant and, without any action, will continue to grow.

It is unclear whether the Agencies have the exceptional capabilities suggested by numerous reports based on the Snowden revelations or have a significant gap in these capabilities as stated by the Home Office and others. A great fear is that they simply have a significant legal gap in their exceptional technical capabilities (and practice). Unfortunately the public just does not know.

It is essential that the review establishes the true facts about capability and that a way is found to provide credible information to inform public debate.

3. Safeguards to protect privacy

It is well-known that in English law there is no right to privacy, and accordingly there is no right of action for a breach of a person's privacy. The facts of the present case are a graphic illustration of the desirability of Parliament considering whether and in what circumstances statutory provision can be made to protect the privacy of individuals.

Glidewell LJ *Kaye v. Robertson* [1991] FSR 62

Since *Kaye v Robertson* the Human Rights Act 1998 has changed English law. However, the ECJ's attempt to safeguard the right to privacy[1] by striking down Directive 2006/24 was defeated in the UK with the passage of DRIPA.

It is noteworthy that Lord Neuberger, the president of the Supreme Court, ended a recent speech with the following observations that are relevant to this review:

"First, I would suggest that, at least in many cases, the right to privacy is not, in fact, really a separate right, but, in truth, it is an aspect of freedom of expression. If I want to do or say something which I am only prepared to do or say privately, then it is an interference with my freedom of expression, if I cannot do it or say it because it will be reported by a newspaper…

The other point arises from the consequences of the astonishing developments in IT: the ease with which information can be transmitted and received across the world, the ease with which words and scenes can be clandestinely recorded, and the ease with which information can be misrepresented or doctored. These developments may make it inevitable that the law on privacy, indeed, the law relating to communications generally, may have to be reconsidered. It undermines the rule of law if laws are unenforceable."[2]

The question of 'safeguards to protect privacy' cannot easily be detached from the question of what we mean by 'privacy' and how this should be addressed in English law.

Clearer basic legal principles – a reconsidered law on privacy and communications – would provide a better context within which Parliament could legislate, and public authorities could operate, in matters of surveillance.

4. Changing & global nature of technology

Internet access continues to widen in the UK with users increasingly engaging in social networking on global platforms like Facebook, selling goods and services, internet banking, making health appointments or using travel related services.

According to the latest figures from the Office of National Statistics (August 2014) in 2014 38 million adults in Great Britain accessed the Internet everyday, 21 million more than in 2006; access via a mobile phone grew between 2010 to 2014 from 24% to 58%; and 22 million households (84%) had Internet access. In 2014 over half of all adults (54%) used social networking and this figure rises to 91% for the 16-24 age group.

According to OFCOM, the proportion of adults who personally own/use a mobile phone in the UK was 93% in Q1 2014.

These figures are significant in a number of ways. They indicate the scope of the privacy impact arising from internet-based surveillance. They demonstrate the pace and scale of technology-related change that can, and has, taken place - most dramatically by the global growth of Facebook from 1m users at the end of 2004 to

[1] See Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

[2] *The Third and Fourth Estates: Judges, Journalists and Open Justice* at the Hong Kong Foreign Correspondents' Club.

1.11bn users by March 2013. Finally, they confirm the huge importance of overseas service providers like Facebook in thinking about UK citizens' communications data.

Other developments including cloud computing, the Internet of Things (IoT), the growth of big data sets and big data analytics are increasing the amount of data available and the potential to analyse it. This trend is beginning to eliminate any meaningful distinction between communications data and content. This has already been acknowledged by the Home Office in the context of web browsing. In Oral Evidence to the ISC (16 October 2012) they conceded that "*the distinction between data and content, you can argue, is muddied in the Internet world*".

Developments in technology are increasingly generating such vast quantities of analysable data that either a 'capability gap' must eventually be allowed to exist or government will commit itself to ever increasing expenditure in pursuit of near total surveillance of the population. The best way to address this may be to establish clearer basic legal principles and to reflect these within a more considered legislative framework.

5. The legislative framework

Over ten years ago, in January 2003 an All Party Parliamentary Group (APIG) published a report of its inquiry into communications data. Amongst other matters it expressed concern about a lack of clarity in the definition of "communications data", a conflict between various statutes, and delay by the Home Office in publishing a code of practice.

APIG's analysis of the conflict between the Anti-Terrorism, Crime and Security Act 2001 (ATCSA), the Regulation of Investigatory Powers Act 2000 (RIPA), the Data Protection Act 1998 (DPA) and the Human Rights Act 1998 (HRA) recommended that the Home Office should drop its plans to introduce a voluntary scheme for data retention under ATCSA. The Home Office did not follow APIG's advice.

The clarity of the legislative framework has not improved since 2003 and this may, in part, be due to the reactive nature of the legislative programme. RIPA was necessary in order to provide the UK with a lawful basis for interception of and access to communications (including communications data) in the light of *Halford v. United Kingdom* [1997] ECHR 32 and the HRA. ATCSA was a response to 9/ll. The Data Retention Directive (2006/24/EC) – heavily promoted by the UK government – was a response to the Madrid (2004) and London (2005) bombings. And various aborted or abandoned legislative proposals like the draft Data Communications Bill (2012) have been associated with various aborted or abandoned government surveillance projects including ID cards, the Citizen Information Project and the Interception Modernisation Programme.

DRIPA itself was, of course, another 'emergency' response – this time to the European Court of Justice (ECJ) judgment of 8 April 2014 in joined cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger (Digital Rights case) which declared the Data Retention Directive (2006/24/EC) invalid. Given that the ECJ struck down the Directive for being disproportionate under the EU Charter of Fundamental Rights and that the Charter rights are similar to those under article 8 of the European Convention, changing the legislative basis (from the Directive to DRIPA) does not alter these facts. It is a form of forum-shopping that is contrary to the rule of law.

It is possible to detect subtle links between atrocity, reaction, the global and changing nature of technology, capability and the inadequacies of the legislative framework (and process) by noting just one aspect of DRIPA. The government has argued that whilst RIPA was intended to apply to overseas CSPs offering services to UK customers irrespective of where those companies were based, DRIPA was necessary "to make that clear on the face of the legislation" (para 15, DRIPA explanatory notes).

One aspect of surveillance legislation that has been of long-standing concern to the Law Society is the absence of explicit protection in RIPA for legal professional privilege (LPP).

In relation to targeted surveillance, guidance which provides for additional oversight where privileged material might be the subject of interception has been published in the Interception of Communications Code of Practice (issued under s71 of RIPA). The code is directed at those public authorities who may seek warrants under RIPA and the provisions of the code may be taken into account by any court or tribunal and by the Interception of Communications Commissioner.

In relation to mass surveillance (communications data) it would appear that the question of legal privilege does not arise since privilege would apply to the content of a communication. However, the absence of any exception under the Data Retention Directive for persons whose communications were subject to 'professional secrecy' was a matter on which the ECJ commented in the Digital Rights case noting that the Directive "does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy." Given the ability to mine communications data to form a picture, laws requiring data retention and permitting its interrogation by public authorities should have an explicit exception for the fact of communications with legal advisers. That is to say, in an age of mass surveillance traditional common law principles of LPP need to be supplemented by broader protections.

The legislative framework for surveillance is complex and, in part, confused. It has often been the product of inadequate public consultation and debate or Parliamentary scrutiny. Its piecemeal development has often been in response to external threats, judicial decisions or technological uncertainty. It needs systematic review and revision.

6. Conclusion

The adequacy of government's surveillance capabilities are unclear. Greater clarity to inform public debate is essential particularly in relation to achieving some degree of assent to large-scale mass surveillance. Technological developments that are already in train mean that some self-imposed, legally enforceable limits on government surveillance will be essential if the UK is not to become a total- surveillance society (it has already been described by many, including a former Information Commissioner as a 'surveillance society').

Basic principles of English law could be developed, as the president of the Supreme Court mooted they might need to be, which would begin to address the new digital world into which we are moving. These principles should inform a less hasty, better informed legislative programme to deliver a more balanced legislative framework. Arguably this programme should be taken out of the hands of the Home Office and given to a public body with some degree of independence from the government of the day.

All this points to one other matter addressed by the current reviews terms of reference: openness and oversight. In 2013 public authorities made over half a million requests for communications data - a figure the Interception of Communications Commissioner said 'has the feel of being too many'. Alongside the sheer scale of global data flows, the vast expenditure on government surveillance capabilities, the ever expanding reach of technology and overarching surveillance laws which the ECJ has found to be in breach of basic human rights, can it be right that the Interception of Communications Commissioner's Office (IOCCO) is currently staffed by two senior appointees, nine inspectors and two secretarial staff?

Oversight of UK surveillance, including the development of proposals for a balanced framework for surveillance, needs to be conducted by a well-staffed, well-resourced and independent public body with the technical and legal expertise that it needs.

October 2014

Liberty

About Liberty

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

Liberty Policy

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

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

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

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

Sara Ogilvie
Policy Officer
Direct Line 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Introduction

1. Liberty welcomes the opportunity to submit evidence to the Reviewer of Terrorism on the regulatory framework governing communications data and interception powers. The *Regulation of Investigatory Powers Act 2000* (RIPA) is a complex piece of legislation governing surveillance by public authorities. It grants extremely broad access to highly intrusive surveillance powers for a wide array of public authorities generally without any prior judicial oversight. From the moment the Act was introduced Liberty has expressed concern over the breadth of power it contains. Similarly, our concerns with the *Data Retention and Investigatory Powers Act 2014* (DRIPA) – both in terms of procedure and substance – are clearly on record. We take no issue with the use of intrusive surveillance powers per se. We do not dispute the importance of targeted surveillance by the security agencies and law enforcement bodies to prevent and detect serious crime. Nor do we dispute the role that lawful and proportionate intelligence sharing between states can play in furthering that aim. While intrusive surveillance will always engage Article 8 of the European Convention on Human Rights (ECHR) as incorporated by the Human Rights Act 1998 (HRA)[1] (right to respect for private life) such intrusion can be justified if it falls within the more serious legitimate purposes set out under Article 8 (e.g. if done to prevent crime and threats to national security), if it is in accordance with law, and if it can be shown to be necessary and proportionate in all the circumstances. Unfortunately, broadly speaking, RIPA and DRIPA do not provide sufficient safeguards to meet this test.

2. In a democracy based on the rule of law, it is imperative that the powers of the state and its actors are set out clearly in law. This is especially so when the State is acting in a manner that may violate human rights, as the ECHR requires that any interference with rights be 'in accordance with law'. It is important not just that there is a sufficiently detailed legislative framework governing the actions of the security agencies, but that there is a shared public understanding of what the law permits. A vague framework that intentionally or unintentionally obscures knowledge of what the agencies are entitled to do, or an out of date framework that cannot be obviously applied to modern technology, is therefore an inadequate and unlawful one. Ensuring that Parliament and the public understand what the security services are permitted to do does not equate to a requirement that those agencies divulge the details of precisely how and when they are surveilling us. But a clear understanding of the absolute limits of what is

[1] Article 8 (right to respect for private and family life, home and correspondence) of the *European Convention on Human Rights* as incorporated by the HRA.

permitted by legislation is essential when the exercise of powers will be done largely in secret. For these reasons RIPA and associated legislation must be repealed and replaced with a comprehensive new surveillance framework.

The human right to respect for privacy

3. Respect for private life has an important tradition in Britain. While for many years it wasn't given legislative expression, Article 8 as incorporated by the HRA now protects the right to respect for private and family life, home and correspondence. The right to privacy is qualified. This means that interference by the state with an individual's privacy can be permitted, but must be legitimate, proportionate and necessary in a democratic society. Proportionality requires that if there is a less intrusive way of achieving the same aim then the alternative approach must be used.

4. The inclusion of privacy in the post-war human rights framework reflects the fact that privacy is essential to human dignity, it is a public, collective and social good, and its protection is essential for the exercise of all other human rights. When privacy is violated by the State harm results, and over time this gives way to other egregious human rights violations. The nature of privacy violations means that the harm is not always apparent or immediately felt. If someone does not know that they have been subjected to unlawful surveillance, the detriment and any consequent disadvantages may not be visible to the individual or the public at large. But just because harm is not yet visible does not mean that it doesn't exist. Some of the harms caused by our inadequate surveillance framework are now only beginning to come to the fore. For example, the availability of classified GCHQ documents to 850000 security contractors (as revealed by the Snowden leaks) demonstrates how blanket surveillance has the potential to undermine security. Similarly, the recent admission by the security services in Abdel Hakim Belhadj's challenge in the IPT that legally privileged material had not only been intercepted but had in at least one instance been disclosed to external lawyers acting on his case demonstrates how disproportionate surveillance undermines the right to a fair trial.[2] The recent revelation that the police routinely use communications data acquisition powers to access the phone records of journalists, circumventing the usual *Police and Criminal Evidence Act 1984* safeguards, shows how easily the current blanket surveillance system can be used to undermine our greatest

[2] Belhadj and Others v Security Services and Others, Respondents' revised response to the claimants' request for further information, published 6 November 2014.

democratic traditions. A free press and the right to free speech is dependent on respect forprivate correspondence.

5. In addition to its original flaws, RIPA has been strained by advances in technology that have changed the way in which people communicate. As a result there is much more information that can be gathered about and from exchanges than previously. Technological developments have also increased the tools available to those who wish to monitor our communications. These two factors mean that there is now greater potential than ever for our privacy to be infringed bysurveillance.

Consistent provision of safeguards

6. A striking feature of RIPA is that it treats the various forms of surveillance in a patchy and inconsistent manner. Part 1 Chapter 1 deals with interception, Part 1 Chapter 2 with acquisition and disclosure of communications data and Part 2 with covert human intelligence sources (CHIS), directed (covert surveillance in a public place) and intrusive surveillance (covert surveillance in residential premises or private vehicles). Under Part 1 Chapter 1, interception powers are granted to a relatively limited list of bodies. Authorisation requires a warrant from the Secretary of State although the procedural safeguards differ dramatically for "internal" and "external" communications. Under Part 2, hundreds of public bodies can exercise powers and a system of internal authorisation for surveillance largely exists, although the *Protection ofFreedom Act 2012* introduced a system of Magistrates warrants for local authorities wishing to access communications data.

7. All forms of surveillance permitted under RIPA involve what can be substantial interferences with privacy. Historically communications data was considered much less revealing than the content of the communication and consequently the protections offered to communications data under RIPA are even weaker than those existing in the interception regime. However as communications have become increasingly digital, the data generated is much more revealing and copious than before, allowing the state to put together a complete and rich picture of what a person does, thinks, with whom, when and where. Often, communications data can be of more use than content: it is vast, easy to handle, analyse and filter; and, it tends to be collected in a consistent manner. It is therefore no longer appropriate to maintain a distinction between the two forms of information. In a recent ruling, which the US Governmentis appealing, a US

District of Colombia judge extended the protection of the fourth amendment to communications data, stating:

"I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high tech collection and retention of personal data on virtually every single citizen for purposes of querying and analysing it without prior judicial approval."[3]

Any residual belief that the collection and acquisition of communications data is a less intrusive or less significant form of surveillance was surely quashed by the admission by the US Government earlier this year that *"We kill people based on metadata".*[4]

8. Equally, the extremely intrusive potential of CHIS and directed and intrusive surveillance cannot be denied. The Court of Appeal has now confirmed that the 'personal or other relationship'[5] that a CHIS may establish includes intimate sexual relationships[6] and the Metropolitan Police is currently facing common law and human rights challenges brought by women who now believe they were subject to surveillance which included long term sexual relationships, marriage and resulted in children. The harrowing evidence provided by these women to the Home Affairs Select Committee inquiry confirms the potentially life-changing consequences that can result from this form of state surveillance.[7] To treat CHIS or directed and intrusive surveillance as any less deserving of the safeguards set out in the rest of this document would be wholly illogical and would do nothing to improve the damaged and fragile relationship between law enforcement agencies and many sections of the population.

---

[3] Klayman v Obama in in the United States District Court for the District of Colombia, 16 December 2013, available at: http://apps.washingtonpost.com/g/page/world/federal-judge-rules-nsa-program-is-likely-unconstitutional/668/ . In his Call for Evidence, the Reviewer indicates that he is intending to look at the position in other countries, particularly the US and Germany for comparative purposes. We advise that in so doing he considers court rulings and ongoing legal and constitutional challenges as well as current legal arrangements.

[4] General Michael Hayden, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metad ata/

[5] Section 26(8)(a) RIPA.

[6] AJA and others v Metropolitan Police Commissioner and others; AKJ and others v Metropolitan Police Commissioner and another [2013] EWCA Civ 1342.

[7] Home Affairs Committee, Undercover Policing Interim Report, 26 February 2013, written evidence available at http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/837/837we01.htm.

Targeted surveillance instead of mass interception and communications data retention

Interception warrants

9. Interception takes place when a person modifies or interferes with a telecommunications system so as to make available the content of a communication being transmitted to a person other than sender or intended recipient.[8] It covers real time or subsequent access to content. Interception hinges on content being made available: no-one needs to read, look or listen to it for interception to occur. Interception applications can be made by a limited list of individuals which includes Director-General of the Security Service, Chief of SIS and Director of GCHQ. Sections 5 and 8(1) RIPA require individual interception warrants for interception of those present in the UK, known as an 'internal' or 'targeted' warrant. An internal warrant must name or describe a person or single set of premises to be intercepted. Section 8(4) and (5) RIPA allow for the interception of 'external communications' - a communication either sent or received outside the British Islands or a communication that is both sent and received outside the British Islands whether or not it passes through the UK in the course of transit. Under 8(4) a warrant for an external communication need not name a person or set of premises and there is no other specific statutory limitation on the scope of the warrant. Recent disclosures made by the security services in the Belhadj case in the IPT revealed that internal GCHQ policies permitted the targeting of legally privileged communications and that on at least one occasion material of this nature was even handed to external lawyers working on Mr Belhadj's case. This raises incredibly serious concerns about the way in which surveillance of external communications operates and the inadequacy of the purported safeguards.

10. There are a number of problems with section 8(4) warrants. The central difficulty is that the power under 8(4) is not a targeted power, but rather an unrestricted power capable of authorising the bulk interception of all communications leaving or entering the country and all communications that take place between individuals outside the British Isles. With no requirement for a human or premises 'target', the scale of potential interception is unlimited and potentially includes the vast majority of global communications. It is only following the Snowden revelations that the extent of bulk interception under 8(4) has come into the public domain. It is now understood that "Tempora" and associated mass interception programmes operate under the purported authority of section 8(4) of RIPA. Under this programme GCHQ reportedly

[8] Section 2 RIPA.

accesses some 21 petabytes of data – the equivalent of downloading the entire British Library 192 times – and handling 600 million telephone events per day via intercepted fibre optic cables.[9]

11. The Government has attempted to argue that bulk interception is not intrusive if it is carried out by machines rather than humans. This is analysis is deeply flawed. There is nothing passive about mechanical State interception of communications and acquisition of communications data. You cannot intercept a communication in a manner that doesn't interfere with privacy just because you claim that human eyes will not see it. Further, the intimate nature and frequency of ordinary people's modern-day internet communications makes the notion of bulk interception even more alarming. Communications intercepted and held by GCHQ under section 8(4) necessarily concern the most intimate types of personal information – thoughts, feelings, conversations, pictures, family videos, information about medical conditions, relationships, sexuality. The most visceral illustration of the intrusion is GCHQs reported Optic Nerve programme which between 2008-2010 collected still images of Yahoo webcam chats in bulk and saved them to agency databases regardless of whether individual users were an intelligence target or not. It is reported that *"in one six month period alone, the agency collected webcam imagery – including substantial quantities of sexually explicit communications from more than 1.8 million Yahoo user accounts globally."*[10] It is reported that bulk interception of Yahoo users was begun because "*Yahoo webcam is known to be used by GCHQ targets*" and that "*rather than collecting webcam chats in their entirety, the program saved one image every five minutes from the users' feeds, partly to comply with human rights legislation*". This is a chilling reflection of how badly the agencies misunderstand their human rights obligations. The documents disclosed reveal GCHQ's sustained struggle to keep the large store of sexually explicit material away from staff eyes but scant regard is paid to the legality and ethics of intercepting and storing this material in the first place. As reportedly noted by GCHQ "…*it would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person*" and the document goes on to estimate that between 3% and 11% of the webcam imagery harvested by GCHQ contains "undesirable nudity". An internal guide reportedly warned analysts "*there is no perfect ability to censor material which may be*

[9] See, for example, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa .

[10] Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, *The Guardian*, 28 February 2014, available at: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

offensive. Users who may feel uncomfortable about such material are advised not to open them" and further cautioned that dissemination of such images would be a disciplinary offence.

12. This central problem is then exacerbated by a series of other flaws, which include the expansive interpretation apparently afforded by the state to terms contained in section 8(4). Despite the fact that RIPA was enacted in 2000, it was only in 2014 in the course of litigation brought by Liberty and others following the Snowden revelations that the Government shared its interpretation of what the term 'external communication' covers. It was revealed that communications 'posted' on a website with a server based outside the UK, such as Twitter, Facebook and Google searches, are counted as external, even if the sender and receiver of the post are both based in the UK.[11] This is an exceptionally broad and counterintuitive interpretation of 'external'. In fact, in an age when a huge number of private communicationstake place social media platforms located in Northern California, this interpretation of external communications does not withstand scrutiny. The distinction between internal and external communications is also widely misunderstood. In a recent evidence session with the Intelligence and Security Committee (ISC), Phillip Hammond MP, the Secretary of State for Foreign and Commonwealth Affairs, appeared to misunderstand a number of key RIPA terms – in particular the distinction between internal and external communications – and appeared confused about how the warrant system for surveillance operates. If a senior member of Government, whose job involves signing interception warrants, is unable to grasp the details of the RIPA regime, it is difficult to understand why members of the public with little exposure to its operation can be expected to do so.

13. Section 5(6) allows conduct authorised by an interception warrant to include authorisation to intercept and obtain communications data for communications not identified in the warrant so far as necessary to do what is expressly authorised by the warrant. As a consequence of the way that the internet works – electronic communications will take that easiest but not necessarily shortest route to their destination – many, indeed possibly the majority of, internal communications, pass outside the UK on route to their destination notwithstanding that they are both sent and received in the UK. The Government admits that itis difficult if not impossible for the security services to distinguish internal and external

[11] Witness statement of Charles Blandford Farr on behalf of the Respondents in Case No IPT/13/194/CH, 16 May 2014, available at: https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%2 0Charles%20F arr%20 on% 20behalf% 20o f %20the%20Intelligence%20Se rvices%201 6th%2 0May%2 020 14.pdf.

communications, so all are intercepted and processed. It is concerning that the will of Parliament in setting out additional safeguards for the interception of internal communications insection 5 can be so easily subverted by use of 8(4) warrants.

14. Section 16 RIPA purports to create additional safeguards to restrict the use of information gathered under 8(4) warrants. However, these safeguards offer little comfort. In particular, 16(2) purports to limit the use of intercepted content by preventing the security agencies selecting material that is referable to an individual who is known to be for the time being in the British Islands. It has been claimed that this prevents the intelligence services from examining information about UK citizens and residents gathered from 8(4) warrants. Howeverthe ambiguous wording offers no guarantees. For example, if the security services suspect but do not know that an individual is within the British Islands can they still search? Can they retain the material and search it when they know the person is out of the country? Further it is easy to effectively search for an individual without using their name by using keywords and other identifiers. To add to this concern, the safeguards of section 16 only extend to interc epted content, not to any associated communications data gathered via interception. This means that even if section 16 does place effective controls on the way in which the security services handle intercepted content, they are not restricted in how they handle communications data gathered at the same time. This has led to fears that the security agencies may consider themselves to have the power to build a searchable database of all intercepted communications data.

15. It is highly likely that the external interception element of the RIPA framework is unlawful on Article 8 grounds on the basis that it is not in 'accordance with law' and is disproportionate. Liberty, Privacy International and Others are currently challenging the legality of 8(4) in a case against GCHQ being heard in the Investigatory Powers Tribunal. Hearings have been held and judgment is anticipated shortly. A previous case, *Liberty v UK,* concerned 'external communications' interception by the Ministry of Defence of Liberty's telephone, fax and email communications between 1990 and 1997.[12] This took place under the pre-RIPA legislation that allowed interception to cover 'such external communications as are described in the warrant'.[13] The European Court of Human Rights found that this was a breach of Article 8 – the power was too broad as it allowed the interception of almost all external communications transmitted by submarine. Yet the replacement framework for 'external interception' under RIPA is strikingly

[12] Liberty and Others v UK 1 July 2008
[13] Interception of Communications Act 1985.

similar in this respect and will almost certainly fall foul of Article 8 on the same grounds. In a Legal Opinion provided to the APPG on Drones, Jemima Stratford QC and Tim Johnston concluded:

"the statutory framework in respect of the interception of external contents data is very probably unlawful...in theory, and perhaps in practice, the SoS may order the interception of all material passing along a transatlantic cable. If that is the case, then RIPA provides almost no meaningful restraint on the exercise of executive discretion in respect of external communications".[14]

16. There is no principled reason for the difference in procedural protection between internal and external communications. The distinction is a hangover from the Cold War when the authorities' focus was on the communications between foreign Governments their agents in the UK. In a digital and globalised world where ordinary people regularly call, text, email and Skype across national borders any outdated notion that 'external communications' are by their nature more likely to be suspicious or less worthy of protection is redundant. There is no reason why a UK resident should have less procedural privacy protection for emails, text messages, phone- calls or web chats sent or made to people abroad than for their domestic equivalents. Maintaining this distinction indirectly discriminates against those who communicate more regularly with those outside the UK, perhaps by reason of nationality, ethnicity, age etc. Affording lesser protection to the communications of those outside the jurisdiction also undermines the universality of human rights and will encourage other states to breach the privacy of British nationals in a similarly casual manner. The UK should lead the way by respecting the basic rights and freedoms of nationals and non-nationals alike. Requests for interception should therefore be specific, targeted and proportionately circumscribed wherever a person is in the world.

17. Aside from the principled dangers of blanket surveillance, the assumption that collection and retention of ever greater data troves reaps security benefits has been shown to be flawed. President Obama's White House appointed review group found that the US program of bulk interception and metadata acquisition "*was not essential to preventing attacks*" and information

[14] Legal Advice by Jemima Stratford QC obtained by Tom Watson, chair of the APPG on Drones, in the matter of surveillance, available at: http://www.tom-watson.co.uk/wp-content/uploads/2014/01/APPG-Final.pdf

needed to disrupt terrorist plots "*could readily have been obtained in a timely manner using conventional court orders*".[15] This finding is supported by research published by The New America Foundation which undertook an analysis of 225 US terrorism cases that have occurred since 11 September 2001 and concluded that the bulk collection of phone records by the NSA "*has had no discernible impact on preventing acts of terrorism*".[16] The study concluded that traditional investigative methods, including the use of informants, community/family tips, are actually far more effective. In Klayman v Obama, Judge Leon found that the US Government was unable to "*cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the government in achieving any objective that was time-sensitive*".[17] Similarly the 9/11 Inquiry Report confirmed that sufficient human intelligence leads had been available to the security services in order to prevent the attack, but that they got lost amongst the chatter.[18] While some in security and law enforcement organisations are naturally hungry for increased information; independent parliamentarians and policy makers should reflect on the broader strategy and assess the value of harvesting overwhelming amounts of information. In the hackneyed needle and haystack analogy, a bigger haystack is not usually required.

Communications data

18. Mass communications data retention and access is currently permitted under RIPA and DRIPA. DRIPA allows a Secretary of State to mandate, by order, the retention by communications companies of 'relevant communications data' including 'all data' for a period of up to 12 months for any of the broad purposes set out in section 22(2) paragraphs (a) to (h) of RIPA. As with external interceptions, RIPA does not require that communications data authorisations specify a named individual or premises, leaving open the possibility that RIPA allows applications for bulk communications data acquisition by public bodies.

---

[15] *Liberty and Security in a Changing World*, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12 December 2013, available at: http://apps.washingtonpost.com/g/page/world/nsa-review-boards-report/674/.

[16] *Do NSA's bulk surveillance programs stop terrorists?* New America Foundation, Peter Bergen, 13 January 2013, available at: http://newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists

[17] See footnote 8.

[18] Report of the National Commission on Terrorist Attacks Upon the United States, available at: http://govinfo.library.unt.edu/911/about/index.htm.

19. Mass communications data retention is undemocratic and unlawful. In April 2014, the Court of Justice of the European Union declared the EU Data Retention Directive 2006/24/EC to be invalid as its provision for the blanket retention of data was incompatible with the rights guaranteed under Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union.[19] The judgment set out the parameters of a fair data retention regime, highlighting for example that retention of data should be targeted at a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences. The ruling also made clear that there should be exemptions from retention in cases involving professional secrecy, such as journalism. The UK's new regime does nothing to address the principled problems with blanket data retention as set out by the CJEU, and Liberty believes it highly likely that DRIPA will be declared incompatible with Article 8 of the ECHR.[20]

20. Government justifies mass communications data retention by reference to its widespread use in criminal investigations and prosecutions. But widespread use of communications data in criminal investigations is unsurprising given that data on the entire population has been retained for several years and law enforcement is able to access the data with ease. In presenting this justification, no detail is provided about the role of historic communications data in the investigation and the proportion of prosecutions that could have been secured without access to bulk historic communications data. Similarly, no regard is had to the huge departure from past practice that this approach represents. Historically, targeted and suspicion-based surveillance has been the norm in the UK, best exemplified by that fact that the Royal Mail has never been required to intercept or keep sender/receiver records of all mail it deals with just in case this information later turns out to be of use to the authorities.

21. Over the past few years, communications data has been accessed on a massive scale in the UK with roughly half a million requests from public bodies per year. The sheer volume of requests and inadvertent examples of bad practice make clear that use and abuse of communications data is a serious problem. In 2013, 869 communications data errors were reported to the Interception of Communications Commissioner and a further 101 identified

[19] Cases C-293/12 and C-594/12, Digital Rights Ireland v Minister for Communications and others (8 April 2014),

[20] Liberty is currently representing two MPs seeking permission for a judicial review challenging the lawfulness of the legislation, see *David Davis MP and Tom Watson MP v Secretary of State for the Home Department.*

during his random inspections. Several errors were reported by him to have had "very serious consequences". The Commissioner warns he is concerned about "*significant institutionaloveruse of the Part 1 Chapter 2 powers*"[21] and has said "*since a very large proportion of these communications data applications come from police and law enforcement investigations, it may be that criminal investigations generally are now conducted with such automatic resort to communications data that applications are made and justified as necessary and proportionate, when more emphasis is placed on advancing the investigations with the requirements of privacy unduly subordinated*."[22]

22. The Commissioner's observations raise concerns not just about privacy infringement but about the impact that mass data retention has on law enforcement policy more generally. In an area of limited resources, excessive availability of data on the whole population is not necessarily a boon for police. There are countless recent examples of situations in which tragedy has resulted from situations where the police had the information required, but failed to prioritise it and respond to it properly. The recently published report of the independent inquiry into child sexual exploitation in Rotherham between 1997 and 2013 demonstrates the huge failure of police to act on information about sexual abuse of children.[23] The report made a 'conservative' estimate that during that time period 1,400 children were sexually exploited, with the report concluding that the 'abuse continues to this day'. The report catalogues the catastrophic failure of South Yorkshire Police to respond to allegations made by young girls, reporting that many victims were instead ignored or treated with contempt by the police. Similarly, in spring 2014, Her Majesty's Inspectorate of Constabulary reported on the police response to domestic violence.[24] It concluded that poor practice often prevents vital information from being placed in the hands of officers quickly and reported that victims had told HMIC that they did not feel believed or taken seriously by the police. There are many examples of the tragic consequences these failures to handle and respond to information.[25]

---

[21] Annual Report of the Interception of Communications Commissioner 2013, para 4.28, published April 2014.
[22] Ibid.
[23] Professor Alexis Jay OBE, *Independent Inquiry into Child Sexual Exploitation in Rotherham (1997- 2013).*
[24] Her Majesty's Inspectorate of Constabulary, *Everyone's Business: Improving the Police Response to Domestic Abuse,* 2014.
[25] For example, Joanna Michael dialled 999 and explained to the call handler that her ex-boyfriend had turned up in the middle of the night, found her with a new partner and attacked her. Her ex -partner had taken her new boyfriend away in his car and had told Joanna that, on his return, he was going to kill her. The call handler graded the call as requiring an immediate response and passed the case over to South Wales Police – however, the call handler neglected to pass on key information, including the fact that

Improvement of Mutual Legal Assistance Treaties (MLAT) to replace Extraterritoriality

23. When law enforcement agencies seek to access information held by or passing through the infrastructure of a company under foreign ownership, the processes for doing so must be lawful, transparent, and contain adequate safeguards to respect human rights. Previous "backdoor" access to such data does not conform to these requirements and neither does a system of voluntary data disclosure. Section 4 DRIPA also does not conform to requirements of transparency and due process and instead creates a novel extra-territorial approach to enforcing surveillance requests outside the jurisdiction.

24. Section 4 sought to extend the territorial reach of RIPA in a number of ways:

- Under section 11(2), where RIPA warrants are served on a person and that person requires the assistance of others to give effect to the warrant, a copy of the warrant may be served on those others. DRIPA allows that even if those others are outside of the UK and the conduct that is required to be undertaken will take place outside of the UK, a copy of the warrant can still be served.
- Under section 12 RIPA, there is a power to require that those providing postal or telecommunications services maintain capabilities so that they are able to comply with requests from the UK Government. DRIPA again extends this power so that it applies to those providing services outside the UK.
- Under section 22 RIPA, public authorities can be authorised to access communications data. DRIPA extends this power so that access to communications data held outside the UK can be authorised under this section.

25. As DRIPA was passing through Parliament, the Government claimed that these were not new powers – rather they were a clarification of powers that already existed. This is simply not the case. In general terms, legislation passed by the UK does not have direct effect in other jurisdictions, just as we would not expect the law of, say, France to apply automatically in the UK. For the Government to claim that RIPA had extraterritorial effect without it even stating so in the legislation is absurd. Where there are difficulties in determining which legal system should apply in certain cases, the system of conflict of laws is applied – it is not simply enough for one

---

Joanna's two children were also in the house. South Wales Police downgraded the call which allowed them up to an hour to respond. Joanna's home was only a few minutes from the nearest police station. At 2.43am Gwent Police received a further call from Joanna. She was heard screaming before the line went dead. Officers then attended and found her stabbed to death.

country to declare that its laws apply in another country. It also contradicts the Government's previous position as set out in the Home Office consultation paper *Protecting the Public in a Changing Communications Environment* which said *"overseas companies outside UK jurisdiction are not required to disclose data under RIPA and not required to retain the data under the EU Data Retention Directive."*[26] This position was confirmed by the joint parliamentary committee that examined the Draft Communications Data Bill in 2012 and said ofRIPA - "*Legislation passed by the UK Parliament does not have direct effect outside the jurisdiction…If the CSP is based outside the jurisdiction only two courses are available to UK authorities requesting the data. The first is to rely on the goodwill of the CSP…The second is to rely on Mutual Legal Assistance Treaties…*"[27]

26. Not only was it wrong for the Government to mislead Parliament and the public as to the effect of section 4 DRIPA, but the consequences of this attempt to extend the tentacles of the British state will have significant and unwelcome consequences. Companies subject to a request to provide information or build up surveillance capabilities will find themselves subject totwo or more different sets of legal requirements and the law of the jurisdiction in which the company is based may prohibit the company from intercepting or building up its capabilities in the way requested by the British Government. This means that it will be for a private company todecide which sets of laws it chooses to comply with in any given case.

27. When extra-territorial provisions were proposed in the Draft Communications Data Bill, the Committee reported that -

"All the overseas CSPs which gave evidence to us had major concerns about the jurisdictional issues, and in particular about overlapping jurisdiction. Stephen Collins from Hotmail said that the Home Office had not explained how it would address the possibility of obligations in the draft Bill putting Microsoft in a position of legal conflict with its home state laws in the USA, Ireland and Luxembourg. Emma Ashcroft from Yahoo! was concerned that extending jurisdiction would set a "global precedent" with the United Kingdom being the first State to adopt provisions of this type. She believed that other States would follow, using legislation to limit free expression and infringe privacy rights. She felt that the draft Bill "would

[26] Protecting the Public in a Communications Data in a Changing Environment, Home Office, April 2009, page 19, available at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_04_09com municationsconsultation.pdf.

[27] Report of the Joint Committee on the Draft Communications Data Bill, November 2012, para 230-1.

create a bewilderingly complex patchwork of overlapping and potentially conflicting laws, andput companies like ours in a very difficult position where we have to make difficult decisions about how to be consistent in our approach to law enforcement and protecting our users." Colin Crowell from Twitter said that there were questions about the assertion of authority over a company subject to US laws…Simon Milner told us that Facebook would "strongly oppose" a measure requiring it to violate the law of another State."[28]

The Committee concluded that *"it would be wrong to use a United Kingdom statute to seek to impose on the on the CSPs requirements which conflict with the laws of the countries where they are based".*[29] Liberty agrees. It is irresponsible for the British Government to put providers in this position and it is completely unacceptable that they should be required to act as the arbiter of human rights, determining whether in individual cases the human rights safeguards required by one country are to be implemented or ignored.

28. The international precedent this creates has further ramifications. If US technology companies are required to enforce UK warrants and requests for communications data then what about warrants and requests from Russia or Saudi Arabia? How would the British Government react to Chinese legislation requiring UK technology companies to comply with its interception warrants or requests to collect communications data held in the UK? These provisions set a dangerous precedent giving the green light to authoritarian States to assert extra-territorial jurisdiction over the interception and collection of our communications. It shows other States that it is acceptable to seek to access information about private citizens without regard for the legal safeguards that may apply in the jurisdiction where the information is located. It is extremely concerning that the Government believes safeguards created by one legal order should be able to be so easily circumvented by another. If companies comply with extra-territorial requests made by the UK in breach of laws elsewhere in the world it will make the UK Government complicit in undermining the rights of individuals both in the UK and abroadand lowering human rights protection internationally.

29. In a globalised and digital world, the provision of communications infrastructure will only continue to be an international, cross-border affair. It is therefore imperative that the UK

[28] Ibid at para 239-40.
[29] Ibid at para 241.

government develops a sustainable, coherent and responsible policy that respects the jurisdiction of others. The alternative, most appropriate – and probably most successful way – for Government to seek to access information held overseas is to extend and improve the use ofMutual Legal Assistance Agreements (MLATs) with other States. MLATs operate under the Crime (International Co-Operation) Act 2003 and allow for the sharing of information between States for the purposes of detecting and prosecuting crime. They provide a transparent framework, avoiding the legal complexities and human rights risks of States seeking to act unilaterally, leaving service providers as the only barrier against privacy violations. Not only do they offer the best way of ensuring that safeguards are applied internationally, but they have the capacity to be an extremely effective method for the transfer of information. The Government has claimed that the MLAT system is too slow and bureaucratic to be an effective tool. However MLATs are wholly a product of Government – the terms are decided by Government, they are implemented by Government and they are funded by Government. It is difficult to see why, with commitment and leadership, inefficiencies cannot be reduced and MLATs turned into a useful, human rights compliant model for information sharing between states.

Establishment of a lawful and transparent framework for surveillance information sharing

30. Outside of MLATs, the power to share surveillance data between the UK and foreign intelligence agencies is currently not provided for in law. While various pieces of primary legislation are in play, none authorise the circumstances in which the security agencies can disclose, request or obtain unsolicited surveillance data to or from foreign intelligence partners. Liberty believes that the current framework is not sufficiently accessible or foreseeable to be 'in accordance with law' nor sufficiently proportionate to satisfy Article 8 and safeguard rights.

31. In the wake of the Snowden revelations, we were concerned that UK agencies effectively circumvent RIPA controls on interception and acquisition of communications data byrequesting or receiving unsolicited, information gathered by the NSA and other intelligence agencies. If so it would effectively undermine the domestic scheme and its already limited protections and– according to the ISC – constitute a "serious violation of the rights of UK citizens."[30] In July 2013 the ISC considered these concerns and concluded: "*in cases where*

[30] Intelligence and Security Committee, Statement on GCHQ's Alleged Interception of Communications under the US Prism Programme, 17 July 2013, paragraph 4.

GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in the Regulation of Investigatory Powers Act 2000."[31] This statement gave the clear impression that UK agencies were bound by RIPA controls when requesting interception data from foreign Governments.

32. However, as a result of the current case brought by Liberty, Privacy International and Others in the IPT, we have learnt via a disclosure from the Government (annexed here) that the UK may request unanalysed bulk data held by a foreign government in the absence of a RIPA warrant. The disclosure does not provide exhaustive detail on when GCHQ believes it is excused from the requirement for a RIPA warrant but offers, by way of example, circumstances where it is "*not technically feasible to obtain the communications via RIPA interception*". The document goes on to state that material received is *"pursuant to internal 'arrangements', subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA."* In the absence of a clear statement in this disclosure that the statutory RIPA safeguards apply, it appears extremely likely that the only "safeguards" that apply are internal ones which are not publicly known. It is concerning that the s16 safeguards which purport to prevent the security agencies from searching a database of intercepted information for individuals known to be within the British Isles do not apply to shared information. This is an extraordinary position which effectively undermines the entire RIPA warrantry system.

33. The impact of this situation is magnified by the scale of surveillance of the UK population permitted by foreign jurisdictions and undertaken by their respective intelligence agencies. In the same way that RIPA inadequately protects the rights of non-UK nationals, the privacy protections offered to UK nationals by the US are weak.[32] Therefore bulk data collected via the mass interception of "foreign communications" by the NSA under its PRISM programme can be

---

[31] Intelligence and Security Committee, Statement on GCHQ's Alleged Interception of Communications under the US Prism Programme, 17 July 2013, paragraph 5.

[32] The Foreign Intelligence Service Act 1978 (as amended in 2008) provides the relevant legal framework for the US interception of communications for foreign intelligence purposes. The Act provides the most limited protection to foreign persons who may be the subject of surveillance or have their communications intercepted and stored by the NSA. Section 702 provides that the US Attorney General and the Director of National Intelligence may authorise jointly, for a period of 1 year the "targeting of persons reasonably believed to be located outside the USA to acquire foreign intelligence information". 'Foreign intelligence information' is broadly defined and an authorisation generally requires an order from the FISA Court, made on an ex parte basis in closed proceedings.

passed to the UK authorities completely outside of RIPA control. The same applies to otherforms of indiscriminate surveillance practiced by other foreign intelligence partners.

34. The framework for disclosure of surveillance data by the UK to foreign agencies is similarly loose and permissive and takes place outside any recognisable legal framework. Transfer of data in this way is a fresh interference with Article 8 and the lack of a statutory framework means that the practice is not in accordance with law. Article 8 further requires that data transfers are necessary in a democratic society and proportionate. The reported scale of UK interception and communications data acquisition under Tempora and the close ties between UK and USA raises the prospect that GCHQ discloses vast quantities of private communications data to the NSA in breach of Article 8. Indeed Guardian reports bear this out –

By May last year 300 analysts from GCHQ and 250 from the NSA had been assigned to sift through the flood of data. The Americans were given guidelines for its use but were told in legal briefings by GCHQ lawyers: "We have a light oversight regime compared with the US."When it came to judging the necessity and proportionality of what they were allowed to look for, would-be American users were told it was "your call". The Guardian understands that a total of 850 000 NSA employees and US private contractors with top secret clearance had access to GCHQ databases.

35. The data-sharing arrangements that we have with the US are made even more significant by the US's well-documented programme of extra-judicial killing. While the British Government has chosen to 'neither confirm nor deny' the allegation that it shares surveillance information with the US to facilitate drone strikes outside of a conventional conflict scenario[33] in a Legal Advice prepared for the APPG on Drones, Jemima Stratford QC considered the positionif the UK were to transfer information that was used to locate and kill 'non-combatants', (as the CIA currently does in Yemen and Pakistan) –

"the transfer of data to facilitate a drone strike is likely to be unlawful for the purposes of English law because the drone strike itself would not be a lawful act, if carried out by the UK

[33] *Khan v Secretary of State for Foreign and Commonwealth Affairs* [2014] EWCA Civ 24. As per Treasury Solicitor *"it would not be possible to make an exception to the long-standing policy of successive governments to give a "neither confirm nor deny" response to questions about matters the public disclosure of which would risk damaging important public interests, including national security and vital relations with international partners."*

government…GCHQ employees providing locational intelligence, that they knew would be used for the purpose of drone strikes are at risk of prosecution as secondary parties to murder."

36. Legal and proportionate arrangements for the sharing of surveillance data between intelligence agencies should be agreed between the UK and foreign counterparts, made publicly available and incorporated into law. This would not require disclosure of any information concerning operations, techniques or capabilities but rather the publication and enactment of a legal framework that will apply to the transfer of individuals' data including that of UK residents.

New requirement for prior judicial authorisation

37. Interception warrants are currently issued by the Secretary of State. Acquisition of communications data by law enforcement agencies and an array of other public bodies is predominantly self-authorising and requires no prior external oversight. Authorisation is simply by a designated person within the organisation seeking the access to surveillance. Authorisation for CHIS similarly requires no prior external oversight.

38. Executive and internal authorisation for state surveillance is unsustainable and should be replaced with prior judicial authorisation. It is the proper constitutional function of the independent judiciary to act as a check on the use of State power. Judges are best suited to applying necessary legal tests to ensure that surveillance is necessary and proportionate and their involvement would improve public trust and confidence in the system of surveillance, so damaged by the Snowden revelations. English law has long recognised the need for judicial warrant before a person's home can be searched by police and there is no longer any meaningful distinction between the quantity and nature of personal information that can be discovered and retained during a premises search and via the surveillance practices permitted under RIPA.

39. The European Court of Human Rights has stressed the importance of prior judicial involvement in State surveillance. In *Klass v Germany* the Court made clear that, in an area where abuse is easy in individual cases and abuses have such harmful consequences for democratic society as a whole, it is desirable to entrust supervisory control to a judge: *"The rule*

of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence,impartiality and proper procedure".[34] More recently in *Dumitru Popescu v Romania (no. 2)*,[35] the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body's activity. David Bickford, former Undersecretary of State and Legal Director of MI5 and MI6 has recently said *"in my view…the extent of covert surveillance today and the pressures involved in its authorisation, particularly on the balances of necessity and proportionality, instruct us that the principle in Klass of judicial authorisation must now be applied."*[36]

40. There is evidence from other comparable jurisdictions that requiring independent judicial authorisation for interception warrants is a workable system. In America,[37] federal investigative or law enforcement officers are generally required to obtain judicial authorisation for intercepting 'wire, oral and electronic' communications, and a court order must be issued by a Judge of a US District Court, US Court of Appeals or FISA judge. In Australia, law enforcement interception warrants must be issued by an eligible Judge or a nominated Administrative Appeals Tribunal judge.[38] In Canada it is unlawful to intercept private communications unless the interception is in accordance with an authorisation issued by a judge,[39] and in New Zealand police can only intercept a private communication in tightly prescribed circumstances, including requiring a warrant or emergency permit that can only be issued by a High Court Judge.[40]

---

[34] *Klass and others v Federal Republic of Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978.
[35] No. 71525/01, § 61, 26 April 2007; 70-73, and cited with approval in *Case of Iordachi v Moldova*, 25198/02, 10 February 2009.
[36] David Bickford CB, European Parliament Libe Enquiry, Judicial Scrutiny of Intelligence Agencies, 7 November 2013.
[37] Under Title III of the *Omnibus Safe Streets and Crime Control Act 1968*, 18 U.S.C. §§ 2510-22, as amended by the *Electronic Communications Privacy Act* (ECPA) of 1986, the *Communications Assistance to Law Enforcement Act* (CALEA), by the *USA PATRIOT Act* in 2001, by the *USA PATRIOT Reauthorization Acts* in 2006, and by the *Foreign Intelligence Surveillance Act (FISA) Amendments Act* of 2008.
[38] *Telecommunications (Interception and Access) Act 1979*, section 39, as amended by the *Telecommunications Act 1997*. Note that Federal warrants relating to national security can be authorised by the Attorney General. See also the various States and Territories that have enacted legislation in order to make the Federal provisions applicable to State and Territory Police, see for example the *Telecommunications (Interception) (State Provisions) Act 1988* (Victoria).
[39] Canada *Criminal Code*, Part VI, section 186.
[40] Part 11A of the *Crimes Act*, and under the *Misuse of Drugs Amendment Act 1978*.

41. As regards communications data, it is entirely unacceptable for public authorities to be able to self-authorise access to revealing personal data. We do not seek to impugn the integrity of public officials or senior employees of our law enforcement agencies, but rather point out the reality that their primary concern will relate to the operational capacity of their agency. This is a matter of organisational culture and is perfectly understandable, but it is also a reality which mitigates in favour of independent third party authorisation. Decisions concerning necessity and proportionality can only be properly made by someone without any conflict, or perceived conflict, of interest. By way of comparison, it is highly unlikely that the destructive surveillance activities of Metropolitan police CHIS would have continued under a system of prior judicial authorisation. This badly regulated practice, based on a system of internal authorisation, has led to collapsed prosecutions and convictions overturned. It has also led to gross human rights violations and untold harm. These scandals demonstrate the fatal problems of internal authorisation as currently permitted for number of RIPA surveillance techniques.

42. The same concerns exist over Executive authorised interception. There is no reason to suggest that any Minister sets out to act in an inappropriate manner. However, the responsibilities of the Executive are diverse and potentially conflicting. There is a wider obligation to the public's safety, to detect and prevent crime and to ensure that state enforcement agencies are able to operate effectively. This range of obligations does not necessarily lend itself to objectivity when determining whether interception is warranted in an individual case. Even if the Secretary of Secretary were to act in a manner of absolute proprietyon every occasion he or she were asked to authorise a warrant, Executive authorisation can lead to allegations of 'rubberstamping'. Without some arm's length independence from the authorising body, there will always be suspicions that proper protocol and safeguards are not being observed. It would be in the interests of both the Executive and the agencies seeking authorisation if an independent judge were required by legislation.

43. Further, issuing warrants authorising the interception of private communications is clearly a very heavy burden to place on a small number of politicians. In 2013, 2760 interception warrants were authorised, or over 7.5 a day (not including the number of intelligence service warrants granted for intrusive surveillance, however many that may be). How a Secretary of State can effectively and properly review high numbers of warrants each day, in addition to his or her other highly pressing duties, raises some serious questions. The

former Home Secretary David Blunkett has recalled the level of pressure he was under when Home Secretary:

My whole world was collapsing around me. I was under the most horrendous pressure. I wasbarely sleeping, and yet I was being asked to sign government warrants in the middle of thenight. My physical and emotional health had cracked.[41]

44. Judicially authorised interception warrants could also pave the way for removal of the ban - enshrined in section 17(1) RIPA – on the use of intercept evidence in criminal prosecutions. There are no fundamental human rights objections to the use of intercept material, if properly authorised by a judicial warrant under a system with adequate safeguards, in criminal proceedings. GCHQ is understood to have resisted efforts to make intercept productadmissible as evidence as such a move would reveal the scale of its interception programmes and lead to a 'damaging public debate'. This serves to highlight how removing the admissibility ban could play an important role in keeping the surveillance activities of the state in lawfulcheck. The Chilcot Review[42], the Joint Committee on Human Rights[43], three former Directors ofPublic Prosecutions[44], a former Attorney General and even the former director of M15 Dame Stella Rimington[45] have reached the conclusion that intercept can and should be used. In the face of this diverse and unlikely coalition of supporters for a change in law, the Government's position on intercept evidence is untenable.

Narrowing of purposes for which surveillance can be conducted

[41] Blunkett: How I cracked under the strain of scandal, *The Guardian*, 7 October 2007, available at: http://www.guardian.co.uk/politics/2006/oct/07/uk.davidblunkett

[42] See Privy Council Review of Intercept as Evidence, 30 January 2008, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228513/7324.pdf

[43] In a number of reports, including Counter-terrorism policy and human rights: 28 days, intercept and post-charge questioning, Nineteenth Report of session 2006-2007 paragraph 32.

[44] Mr Keir Starmer QC, Oral Evidence of Director of Public Prosecutions, Keir Starmer QC to the Home Affairs Select Committee; Lord Ken MacDonald QC,: Law Society Gazette, 'Human rights lawyers back Goldsmith call to use intercept evidence in court', 28 September 2006; Sir David Calvert -Smith QC: The Observer, 'Juries should hear phone taps to nail crime gangs'.

[45] Guardian, "Courts set to admit wiretap evidence", 21st September 2006

45. The purposes for which RIPA powers can be granted are broad and ill-defined. Section 5 RIPA requires that interception warrants may only be issued where the Secretary of State considers it necessary and proportionate to do so in the interests of national security; the prevention and detection of crime; or in circumstances relevant to the interests of national security to safeguard the economic wellbeing of the UK. These terms are also used at sections 15 and 16 RIPA to regulate the use of material once it has been intercepted. As such, they are one of the key safeguards in the intercept regime. These terms are not objectionable at face value and they are clearly intended to reflect the language of necessity and proportionality contained in the HRA. They are, however, exceptionally vague and broad terms and give the Home Secretary a huge discretion. As there is no appropriate judicial approval given before these powers are exercised, whatever the Home Secretary subjectively decides is in the interests of national security or the economic well-being of the UK is what will be used to authorise the surveillance. The use of broad and vague notions such as 'national security' and 'economic well-being' gives rise to a real risk that the disproportionate use of surveillance will be authorised, going beyond what is necessary to protect the public from harm. This could interfere unacceptably with political and other lawful activity that ought to go unimpeded in a democratic society. We believe that these grounds should be better defined, particularly as the prevention or detection of crime, or serious crime, is already included which should capture the majority, if not all, of the grounds on which surveillance needs to be authorised.

46. Sections 22(2)(a) to (h) RIPA set out the purposes for which communications data may be required to be retained under DRIPA and then accessed by a wide range of public bodies. The list includes the purposes set out in section 5 but is much more extensive allowing retention and access of communications data for the purpose of preventing or detecting *any* crime, assessing tax or any levy or charge payable to a government department, preventing disorder, or in the interests of public safety. The Secretary of State also has the power to make orders extending the purposes for which authorisations can be made. In view of the rich and comprehensive picture that can be painted by communications data, this long and broad list of purposes is very worrying. The grounds for which RIPA allows surveillance have clearly been chosen as they are the main grounds on which the right to privacy under Article 8 of the HRA can be limited. However, just because they form grounds on which this right *may* be limited where it is necessary and proportionate to do so, this does not mean that targeted surveillance can be justified for all these purposes. On the spectrum of intrusions into the private sphere, state surveillance is already at the more intrusive end. Further, a number of the purposes do not

even fall within the Article 8 justifications and the ability of the Secretary of State to expand thelist by an order also contrasts with the prescriptive nature of Article 8.

47. In the recent Digital Rights Ireland case, the Court of Justice of the European Union set out that retention of data should be restricted to purposes related to ensuring public security and access and use of data should be restricted to purposes concerning the prevention, detection or prosecution of defined, sufficiently serious crimes. The list of purposes for whichcommunications data can be acquired under RIPA should be amended accordingly to restrict access to the prevention and investigation of serious crime and the prevention of death and injury. What constitutes 'serious' crime is defined in RIPA and the 1997 Act as being an offence that involves violence or results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose or is an offence for which a person could be reasonably expected to be imprisoned for three years or more.[46] This is a generous definition of serious crime and it is difficult to see why surveillance under RIPA should be permitted in order to detect non-serious crimes. In making this argument we do not suggest that non-serious crimes should not be properly investigated, rather, there is a need to explain why other methodsof investigation and enforcement cannot be used in such circumstances.

48. This reform will necessarily require a welcome restriction on the public bodies authorised to access such data. Many hundreds of public bodies are currently authorised to access communications data as a result of successive orders made under section 25(1). [47] These include local authorities as well as bodies as diverse as the Charity Commission and the Pensions Regulator to name just a few. A large number of the bodies listed play no role in the prevention or investigation of serious crime nor the prevention of death and injury.

Redress for individuals subject to unlawful surveillance

[46] See section 81(2) and (3) of RIPA and section 93(4) of the *Police Act 1997.*
[47] For a list of bodies with the power to self-authorise the acquisition of communications data see the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI No 480).

Disclosure

49. Section 19 of RIPA makes it an offence for state officials to disclose the existence and contents of a warrant to intercept communications. Disclosure of the use of other surveillance mechanisms is not prohibited, but nor is it required, other than to the relevant Surveillance Commissioner who must report in general terms on its use. Therefore, a person subjected to surveillance is unlikely to ever be made aware of that fact unless they are told by the relevant public authority of the surveillance. As Liberty submitted in its second reading briefing when RIPA was introduced as a Bill in 2000:

The individual's right to complain of an infringement of rights is reduced to a matter of chance – for example, the individual might become aware of interception only after a security service leak. Scrutiny arrangements such as those envisaged by Part IV can only work effectively if those affected by interception are given notice as soon as practicable (usually after completion of the investigation) that it has been carried out.[48]

If a person's Article 8 right to privacy has been infringed, in order to have access to an effective remedy as required under human rights law, the person must first be made aware of a possible breach. This was stated by the European Court of Human Rights in *Klass v Germany* in 1978 and reiterated in *Weber and Saravia v Germany* in 2006:

The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see Klass and Others, cited above, pp. 26-27, § 57).[49]

We believe that once an investigation has been completed, or once that person is no longer under any suspicion, he or she should be notified of the relevant surveillance unless there is a specific reason for maintaining secrecy.

[48] Liberty, Regulation of Investigatory Powers Bill: second reading briefing, House of Lords, May 2000, page 3, available at: http://www.liberty-human-rights.org.uk/pdfs/policy00/may-2000-ripa.pdf
[49] *Weber and Saravia v Germany*, 2006, application 54934/2000, paragraph 135.

Investigatory Powers Tribunal

50. Legal challenges against the use of the surveillance powers under RIPA are heard by the Investigatory Powers Tribunal (IPT). The redress offered by the IPT is inherently limited. It is exceptionally difficult for an individual or organisation to bring a credible case to the tribunal, because to help formulate a claim that person needs to have a very good suspicion or evidence that they are under surveillance. Given the inherently secretive nature of surveillance, very few are in a position to do this. As there is currently no requirement to notify individuals who have been subject to surveillance, instances of unlawful surveillance will go largely unknown and unchallenged. Indeed, Liberty's current challenge in the IPT – to the section 8(4) safeguards – was only made feasible by the Snowden revelations. It is instructive that in the first 10 years of the IPT's existence, it upheld a total of ten complaints, five of which concerned members of the same family, represented by Liberty, who complained about local authority surveillance that the authority actually admitted.

51. Those who are able to start a claim in the IPT then suffer from the secretive nature of the Tribunal's procedure. For example, the Tribunal is not required to hold oral hearings; hearings do not need to be *inter-partes*; it cannot disclose the identity of a person who has given evidence at a hearing or the substance of the evidence unless the witness agrees . If the Tribunal finds against a complainant it cannot give its reasons for doing so, meaning that the individual does not know whether no surveillance took place or whether lawful surveillance took place, and if it upholds a complaint is it only required to provide the complainant with a summary of its reasoning. There is no right of appeal from the IPT. This effectively means that in most cases in which a person seeks to argue that a public authority has used unlawful surveillance against them, they are required to bring proceedings before the IPT, which may not hold an oral hearing, will not give proper reasons for its findings and against which there is no right of appeal. This is arguably a breach of Article 6 of the HRA itself which requires a fair and public hearing, and the right under Article 13 of the ECHR to an effective remedy. The IPT must be reformed to make it more open and transparent. It is difficult to understand why the tribunal should not operate on a presumption of open proceedings, with the option for the tribunal to determine that closed or partly closed hearings are in the interests of justice. There should also be the option for parties to appeal the decision of the IPT to a higher court. As with the Commissioners, the IPT could improve the overall transparency of the surveillance system by publishing more detailed statistics about the applications it receives and the cases it hears.

Democratic oversight

Legislative scrutiny

52. In a democratic country it is for Parliament, not the Executive or the security agencies themselves, to determine the extent of surveillance powers. Against the backdrop of the technological revolution it may seem a difficult task, but if Parliament abandons this responsibility, either by declining to reform the law when technological development supersedes it or by reforming it with further opaque legislation riddled with loopholes, it will undermine itsown role as the body the public hold accountable for devising the law. Any attempt to "future proof" legislation results in the bypassing of parliamentary and public scrutiny. As such it is deeply undemocratic and is particularly pernicious when individuals have little ability to know if their privacy is being breached by the state. The new legislative framework must be drafted in sufficiently specific terms, based on our present understanding of technological capabilities. Astechnology progresses and the security services wish to interpret their powers in ways that Parliament couldn't have foreseen, they must be required to return to Parliament to be granted clear powers.

Intelligence and Security Committee

53. Liberty has lost confidence in the ISC's ability to provide effective oversight of the security agencies. We consider that the Committee lacks the necessary resource, inquisitive spirit, specialist knowledge and independence of mind to conduct neutral and informative scrutiny of the security services. The practical failings of the Committee have been identified by others. In Lady Justice Hallett's Coroner's Report from the Inquest into the 7/7 bombings she reported that *"The ISC may have inadvertently been misled and thus …it's reports may not havesufficiently addressed some of the central issues before it."*[50] The Joint Committee on Human Rights noted that the Committee accepted *"apparently without challenge"* the account given by the security services of the treatment of Guantanamo detainee Binyam Mohamed.[51] It later came to light that the security services had been complicit in his ill-treatment. The Joint

[50] Coroner's Inquests into the London bombings of 7 July 2005, paragraph 115.
[51] Joint Committee on Human Rights, Allegations of UK Complicity in Torture, Twenty third report of 2008-2009, paragraphs 60 and 61.

Committee on Human Rights has also noted that *"it can be difficult to follow the Committee's work and to understand its reports"* and the Home Affairs Committee has recently concluded *"we do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability andto the credibility of parliament itself."*[52]

54. The Justice and Security Act 2013 made a few small changes to the ISC, however further changes must be made to membership, powers and resourcing in order to strengthen the Committee and to provide an effective oversight mechanism. The Home Affairs Select Committee has recommended that the ISC chair should be a member of the largest opposition party and the members should be elected by the relevant House not appointed. At the moment, members are elected but candidates are only put forward for selection on the recommendation of the Prime Minister. This should no longer be the case. The Committee should have powers tocompel the production of information and should have control over its own publications, rather than being subject to Home Office control over redaction of reports.[53] The Review may also wish to consider the role that other parliamentary committees could play in holding the security services to account. Earlier in 2014, a request by the Home Affairs Select Committee that the heads of the security services attend an evidence session with the Committee was denied by the Home Secretary. Given the powers of the security agencies over the rights of people in the UK, it is unclear why they should not be made accountable to the Joint Committee on Human Rights and the Home Affairs Committee.

The Intelligence Commissioners

55. There exist a number of commissioner positions which are designed to provide after the event oversight of the use of surveillance powers. Sections 57 and 59 RIPA establish the Intelligence Services Commissioner and the Interception of Communications Commissioner. Both these roles report to the Prime Minister and lay an annual report before parliament. In the

[52] Home Affairs Select Committee Report on Counter-terrorism, Seventeenth report of Session 2013- 2014, paragraph 157.
[53] See Home Affairs Select Committee Report on Counter-terrorism, Seventeenth report of Session 2013-2014, paragraphs 145-157.

absence of prior judicial authorisation, this oversight should offer comfort that surveillance powers have not been misused. Unfortunately, evidence suggests that the systems in place arenot sufficiently robust.

56. In its recent report on counter-terrorism, the Home Affairs Select Committee expressed concern that the Interception of Communications Commissioner inspects only between 5-10% of applications made each year and the Intelligence Services Commissioner had examined only8.5% of warrants. The Commissioner posts are only part time, which may account for the fact that so few investigations are conducted, but it remains the case that these are tiny proportions and conducting investigations into this amount of work offers no guarantee as to the health ofthe system in general.

57. Very recently, in the light of revelations that the police have been using RIPA powers to access communications data records of journalists in order to identify their sources, the acting Interception of Communications Commissioner launched an investigation into this practice. While this investigation is to be welcomed, it is a damning reflection of the system of oversight that at no previous point has the Commissioner's office identified or investigated these extremely worrying practices.

58. After the fact oversight cannot match the protection offered to privacy by prior judicial authorisation and an effective judicial avenue for redress. However, the Commissioner positions can certainly be improved. Thought should be given to the recommendation of the Home Affairs Select Committee that the positions should be made full time and given sufficient resources to undertake a more substantial review of the work of the agencies. The Commissioners could also help others to hold the security services to account by publishing statistics, such as the numberof annual requests for warrants and authorisations granted.

Conclusion

59. The need for reform of the surveillance framework has never been more pressing. Not only is RIPA inadequate in terms of the safeguards it provides and in the way it is used with reference to modern technology in a way unforeseen by Parliament when legislating, but there is increasing evidence that even the limited protections offered by RIPA are circumvented by the security services through information sharing with foreign agencies. The fact that this

understanding of the way in which the security agencies operate has only emerged through the Snowden leaks and subsequent legislation raises significant concern as to the effectiveness of oversight mechanisms.

60. The surveillance legislative framework must now be redrafted to offer consistent provision of safeguards to equivalent but different sources of information; to provide for targetedrather than mass surveillance; to require information sharing between states through MLATs rather than via extraterritorial provisions in domestic legislation; to ensure that additional agreements for information sharing between security agencies are transparent and do not allowthe agencies to circumvent safeguards set out in other parts of the framework; to require prior judicial authorisation for surveillance; to narrow the purposes for which surveillance can take place; and to offer improved oversight and redress mechanisms.

November 2014

Local Government Association

This submission provides information relating to local councils' use of communications data. It has been prepared by the Local Government Association on behalf of all councils in England, and endorsed by the Welsh Local Government Association, in relation to their members in Wales who are dealing with the same issues.

An annex to this document includes a number of case studies (collated by the LGA and National Anti-Fraud Network) outlining how councils have made use of communications data.

Current position

Councils are entitled to access communications data – that is telephone and internet billing and subscriber information, but not the content of any communication – with the judicial approval of a Magistrate, where it is required for the purpose of preventing or detecting crime or preventing disorder. With effect from December 2014, any council wishing to do so will be required to be a member of the National Anti-Fraud Network, a council run shared service that supports its members to acquire data legally, efficiently and in accordance with best practice. Councils do not have powers to intercept communications and the responses below therefore do not address the issue of interception powers.

Councils are not seeking any changes to their communications data rights.

Specific questions and responses

What are the threats and risks with which you are dealing?

Councils may use communications data to tackle a wide range criminal activity. Typically, they will use it as part of their enforcement role in relation to fraudulent activity that is directed at individual consumers, companies or institutions (including the council, such as benefit fraud). This activity may range from doorstep criminals preying on vulnerable people (particularly the elderly) to large scale cyber-crime conducted remotely; what it has in common is that these offences can cause very significant financial loss and deep distress to the victims, as well as the people close to them.

Additionally, communications data may also be used to tackle criminal behavior that impacts on communities, for example environmental crime.

It is important to be clear that councils will almost always invoke these powers in relation to *actual* events and harm that has already occurred, as distinct to using them to *prevent* threats and risks from causing harm. Councils will use these powers to bring the perpetrators of criminal activity to justice, and to prevent further harm from occurring to others through the same activity. This is clearly different to the rationale that other enforcement bodies will sometimes have for using these powers, which is more clearly focused on prevention. However, it is the nature of councils' enforcement role (particularly in trading standards) that an offence is likely to have been committed before a council would seek to invoke these powers in the course of investigating it.

How do you use communications data and interception to address those risks and threats? It would be helpful if you would distinguish the use of communications data, making clear what you regard as such data, from the use of interception and discuss the significance of each in dealing with the threats and risks you are tackling.

Subject to receiving judicial approval from a Magistrate, councils may use communications data for the purpose of preventing and detecting crime and preventing disorder. Communications data is: telephone service user details, call records, and billing information, as well as service user details for internet and email accounts.

As stated, councils use this information to build criminal cases against individuals accused of committing criminal activity and hence to prevent further crimes. In doing so, councils work closely with the police and other partners in the criminal justice system to target resources efficiently and effectively.

Communications data may be used to identify the person owning an email or internet address or telephone number linked to criminal activity. Similarly, in many of the case studies in annex 1, communications data including an individual's home address had enabled councils to trace individuals suspected of criminal activity who had moved during the course of an investigation. It can also be a crucial piece of evidence proving that contact took place between the accused and the victim, and sometimes linking the accused to wider criminal networks. This information can be a vital piece of evidence that substantiates a prosecution case where records may - intentionally - not have been kept, been fabricated, or been destroyed, and where the alleged offender lies about their activities. Without access to this information it would often be impossible for councils to build a criminal case.

The case studies at the end of this submission illustrate how councils use communications data.

What is your projection of how the threats and risks will develop in the future; and what do you see as the future significance of communications data and interception in dealing with them?

Communication increasingly takes place electronically – notably using mobile phone and email, rather than through mail and / or face to face meetings – and this trend will continue, meaning that access to communications data will be an important source of information and evidence where the outcome of such communication leads to harm to individuals or organisations. Regrettably, it is widely accepted that alongside this trend, there will be also be a continued trend towards cybercrime that targets individuals through email and the internet, as well as by phone. By cybercrime, we mean websites that defraud consumers by offering goods or services that do not materialise, or that charge them a price for something that is unnecessary.' In the UK, Norton estimate that more than 12.5 million people fell victim to cybercrime over the past twelve months. The cost of these cybercrimes was a massive £1.8 billion with an average cost of £144 per cybercrime victim.[1]

This type of crime is increasingly sophisticated, and can catch out even individuals who consider themselves to be aware of and alert to these risks. On that basis, communications data will have a continued and increasingly significant role as a key tool for councils (and others) in attempting to tackle this activity and achieve restitution for victims. Without the power to access communications data, it will be extremely difficult for councils to take effective action against criminals committing this type of crime.

[1] Norton Cybercrime Report, September 2012

What are the alternatives* to *using communications data and interception* to *the extent* you *now* do or *envisage in the future? What are the pros and cons* of *using such alternatives?

There are alternative tools (for example, physical observation) that it may be possible to use in relation to certain types of physical, environmental crime, albeit these are tools which may be more resource intensive and not always as cost effective.

However, this is emphatically not the case in relation to cybercrime. When the key weapons of criminal activity are electronic and / or phone based, it is essential that equivalent tools can be used to tackle it. Put simply, there are no alternatives to using communications data to tackle criminal behavior perpetrated through the internet or telephone, including from outside the UK; information gleaned thro.ugh communications data is an essential foundation for successful criminal cases for these crimes. Therefore, while councils are not seeking an extension of their powers in relation to communications data, it is extremely important that the status quo and their existing powers are maintained. Continued access to communications data will enable councils to work closely with the police and others to make the most effective use of reduced resources in order to target specific types of crime.

What are the communications data and interception capabilities that you need* now *and in the future? It would be helpful if you addressed the types of communications and associated data that you will want to examine andthe period* of *time for which the information should be available before therequest to examine it.

The needs of council enforcement teams may change over time as new forms of criminal activity and scams emerge, but councils are not seeking any additional or different powers in relation to communications data at the current time. However, it is imperative that councils' existing powers are preserved, if councils are to be able to effectively undertake their enforcement responsibilities in relation to trading standards, fraud and so forth.

What arrangements do you believe are appropriate* to *enable the communications data and interception needs that you identify to be met whilst minimising the intrusion into the privacy of those whose informationyou are examining?

We believe that the current framework provides an appropriate balance between minimising intrusion into the privacy of those whose information is being examined and the need for councils to take effective action against criminal activity. Therefore, we would like to maintain the status quo and are not seeking any additional powers.

It is important to recognize in considering this balance that, firstly, councils are unable to see the content of any communications; and secondly, that councils will only seek to use their communications data powers in relation to individuals whom they suspect of serious and actual criminal activity (as distinct to criminal *intent).* Applications to acquire communications data will only be made where there is reason to suspect an individual of involvement in criminal activity and acquiring the data is necessary and proportionate to assist in proving, or indeed disproving, their involvement. This power is therefore used sparingly; in 2013, less than 1% of approved communications data applications were made by councils.

In that context, we believe that the involvement of Magistrates and new requirement for membership of NAFN offer the right safeguards to provide publicreassurance that this power is not being misused.

On a related point, we would add that government has a role to play in myth

busting media scare stories in this area. Councils do not use these types of powers to snoop on local residents and their bins, or their dogs: they use them to tackle hardened criminals who prey on vulnerable people and ruin lives. It would be helpful if governments could acknowledge this and rebut some of the scare stories, rather than risk undermining councils' very important reasons for accessing this information.

Is there anything that significantly distinguishes the threats and risks faced by the United Kingdom and the part played by communications data and interception in dealing with them from the situation in other developed democratic countries?

Enforcement and local government structures vary significantly across the developed world and we are unable to offer any detailed comment on this point. However, we note that in a globalized world where at least some of the fraud and crime investigated by councils originates from other countries (whether committed by individuals with links to the UK or not), it seems unlikely in relation to councils' areas of responsibility that the challenges and role of communications data would differ significantly in other developed countries.

Case studies: how councils make use of communications data to stop criminal activity and bring the perpetrators' to justice

Operation Magpie - Cambridgeshire County Council

Operation Magpie concerned an investigation into an organised crime group who defrauded elderly and vulnerable people. The criminals exploited their victims to the extent that one person was evicted from their home, as well as laundering cheques to the value of £700,000.

The ringleader of the gang received a prison sentence of 7 years with two co-conspirators receiving sentences of 5 years each. 16 other offenders were also convicted of money laundering offences serving prison sentences of up to 30 months.

Malcolm Taylor from Trading Standards at Cambridgeshire County Council said "Without access to communications data, we would not have been in a position to connect the conspirators and detect the level of criminality that extended to over 100 vulnerable and elderly victims, some of whom have since died".

Operation Troy - Suffolk County Council

Operation Troy was a long running advanced fee fraud case that was investigated and prosecuted by Suffolk's trading standards service. The fraud operated between 2007 and 2010, involved at least £7.5 million of consumer detriment affecting well over 16,000 consumers and involved two distinct frauds;

1. An escort/companion fraud in which consumers were offered guaranteed work as escorts and companions in return for a registration fee, however no work was subsequently provided.
2. A debt elimination fraud in which consumers paid an advanced fee to receive a debt elimination service but little or no service was ever provided.

The fraud was complex and well organised, operating from call centres in Spain. UK customers made contact with the call centres using free phone numbers that appeared to

be UK based after viewing various escort websites offering work. During calls with escort agency staff, false promises would be made regarding the immediate availability of work and potential earnings available. Many consumers complained of similar experiences and provided similar accounts of last minute cancelled work appointments after they had paid their fees.

The escort websites and telephone numbers changed frequently to confuse consumers and make it difficult for enforcement bodies to track the source of the fraud. By using RIPA powers and obtaining communication data for the telephone numbers used for the fraud, the following links were established:

- The multiple telephone numbers were owned and operated by only two individuals. One of those individuals, who held the majority of the numbers, had been identified as being involved in operating multiple UK bank accounts used for money laundering aspects of the fraud and the creation of shell companies.
- All the UK free phone numbers were being redirected to Spanish based numbers that were linked to a small number of call centres operating from the Malaga area of Spain. These call centres were all owned by one man who was known to have a previous history of fraudulent trading.
- The link provided by this communication data provided evidence that what appeared outwardly to be over 12 different separate escort websites/agencies were in fact all one fraud perpetrated by one set of linked individuals.

In June 2012 European Arrests warrants were applied for in respect of Antoni Muldoon the man at the helm of the fraud, and two other members of the gang, Geraldine French and Bradley Rogers. All three were returned to the UK. Following extradition in September 2012 Muldoon pleaded guilty to conspiracy to defraud at Ipswich Crown Court.

Following Muldoon's plea, and after a series of trials at Ipswich Crown Court including a ten week trial involving five of the defendants that concluded in June 2013, seven further members of the gang were found guilty of offences including conspiracy to defraud and money laundering offences. The sentences handed down totalled 36 years overall, with Muldoon receiving 7.5 years for his role and Mark Bell of Ipswich, Muldoon's right hand man in the UK, receiving 6.5 years.

Confiscation proceedings followed the sentencing and to date £315,000 has been awarded in confiscation and costs, which Suffolk Trading Standards has used to repay victims of the fraud. Confiscation proceedings are continuing against Antoni Muldoon who is known to have benefited to the largest extent from this fraud and the amount of confiscation possible from him is expected to be substantial. Confiscation hearings for Muldoon are set to take place in January 2015.

In July 2014 four of the defendants appealed their convictions and sentences at the Court of Appeal in London and in front of three sitting High Court Judges all appeals were turned down.

Steve Greenfield, Suffolk's Head of Trading Standards and Community Safety commented that 'RIPA powers were essential to the successful outcome of this case.'

Counterfeit goods case study 1

Two internet traders based in Slough were selling **counterfeit trainers** on e-bay for £35.00. The only intelligence the trading standards service had was the e-mail address and mobile

phone numbers that the complainants used to make he purchase. The actual retail price of these trainers was £135 a pair. By obtaining the data from the mobile phones and the I.P address the council were able to pinpoint the address being used by the perpetrators. A test purchase had been made prior to a warrant being sought. A sting operation resulted in a seizure of trainers with a **street value of £325,000** and both offenders received a custodial sentence. Without the communications data this would not have been possible.

Counterfeit goods case study 2

Officers seized some potentially counterfeit mirrors from a shop. By the time the mirrors were confirmed as being counterfeit the trader had disappeared after failing to attend for interview. The contact details he provided proved to be false. However, officers obtained a mobile number for the trader and the subscriber details identified his home address in Swansea. This enabled officers to contact him. He subsequently pleaded guilty to 3 offences under the Trade Marks Act. Without the access to the communications data officers would not have been able to find the new address to which he had moved and so the investigation would not have been able to proceed.

Barnet council - rent deposit scheme fraud

A man and woman were jailed following a Barnet Council investigation to crack a highly organised plot to obtain fraudulent payments from the authority by using a complex web of false identities to open a string of bank accounts which were then activated to receive thousands of pounds in fraudulent rent deposit scheme payments. The rent deposit scheme is used by the council to provide people in need of housing with initial financial support to help secure a tenancy for private rented accommodation.

The investigation by the council's Corporate Anti-Fraud Team (CAFT) was launched after uncovering irregularities with a number of rent deposit payments. Investigators went on to identify 41 fraudulent payments worth £132,629 which had been paid to different bank accounts. During the course of the investigation a further 12 fraudulent payments worth more than £31,600 were intercepted and blocked by CAFT.

CAFT worked with NAFN to obtain mobile phone records, under the Regulation of Investigatory Powers Act, which provided significant evidence to show that the accused were in regular contact on the days when substantial withdrawals and deposits were made..The powers also enabled the investigators to identify the real owners of the false identities by obtaining the mobile phone service providers records which identified names and addresses where these suspects could be found. The legislation also allowed information of redirected post from credit card companies, banks and online purchase deliveries which also assisted in tracing addresses that the suspects used which were then the subjects of police / CAFT raids. Without access to this information the investigation would not have proceeded to a useful outcome.

Landfill tax fraud

A council was alerted to a skip hire company who were disposing of waste in an unauthorised manner, including avoiding payment of landfill tax estimated at £1 .3 million. Enquiries made by the council identified three suspects but there was no evidence to link them to the offences. Subscriber and itemised billing data provided by NAFN proved that there were regular communications between the individuals during periods in question. Without this information, it would have been impossible to pursue a prosecution.

Fraudulent car trader

A car trader was convicted of multiple offences contrary to the Fraud Act 2006 in relation to the sale of misdescribed and clocked cars. Vehicles were purchased at auction with higher mileage and advertised online via AutoTrader. The trader claimed a third party was responsible and he simply allowed the third party to use his account at auction to obtain vehicles more easily. However, SIM cards found in possession of the car trader were confirmed, using communications data, as being associated with unregistered PAYG telephone numbers used in adverts for vehicles. During the course of the investigation, the trader sold his house and moved location; a second set of communications data (forwarding address details from Royal Mail helped to locate him for the purposes of arrest, entry warrants and interview. The penalty was 12 months imprisonment and a Proceeds Of Crime Act confiscation order in excess of £58,000.

Further case studies are available if this would be helpful.

October 2014

Ray McClure

I am the eldest brother of Lee Rigby's father, Phillip, and I have read the “Report on the intelligence relating to the murder of Fusilier Lee Rigby” and would like to make a couple of observations for your consideration in your review of terrorist legislation.

1. “**Report on the intelligence relating to the murder of Fusilier Lee Rigby” states in section 457 “The number of different forms of communication now available presents the Agencies with significant challenges in terms of their ability to detect and prevent terrorist threats to the UK. However, the real problem arises from the fact that most of these services and applications are hosted overseas.” “CSPs based in the US have, for the most part, refused to recognise UK legislation requiring them to provide the content of communications on their networks: they do not consider themselves to be bound by the legal obligations set out in RIPA, as UK CSPs do, and may find themselves subject to legal or civil action if they share information with the UK authorities.”**

   “The considerable difficulty that the Agencies face in accessing the content of online communications, both in the UK and overseas, from providers which are based in the US – such as Apple, Facebook, Google, Microsoft, Twitter and Yahoo – is therefore of great concern.”

   The problem here is actually bigger than this. Today with cloud based storage, a person in one country e.g. UK, is probably using internet services from a another country e.g. USA and the data can be stored in a number of other countries e.g. Ireland.

   This throws up international legal issues as highlighted last year, when Microsoft refused to handover emails to the US government. New York judge James Francis said that a warrant for online information was the equivalent of a subpoena and had to be obeyed. Microsoft and its supporters argue that the centre in Dublin is outside US jurisdiction, while the prosecutors claim that as the data itself is accessible by the firm from within the US, this does not apply. (as reported by the BBC 16/12/14).

   I hope your review can find a solution to this problem.

   The public do fear the big brother syndrome of government monitoring. One parallel from the banking industry which may be worth considering is Anti Money Laundering Regulation. Here the banks are obliged to monitor transaction and if suspicious they must report the transaction to the authorities. The banks are carrying out the monitoring not the government, and they face massive fines and business damage if the fail to do so.

2. The report also states **“that several of the companies attributed the lack of monitoring to the need to protect their users’ privacy. However, where there is a possibility that a terrorist atrocity is being planned, that argument should not be allowed to prevail.”**

   While the real problem here is the wording of the American Constitution which recognises the right to privacy but not the right to life, I strongly feel that the The European Human rights legislation can be improved.

   The European Human rights put Life first. Article 2 protects the right of every person to his or her life, and gives the state a positive duty to prevent foreseeable loss of life. However, while this implies that the right to life takes priority, it does not state it. A simple amendment to

explicitly state that the right to life takes priority over the other rights, especially the right to privacy will add clarity and remove the defence of protecting users privacy where life is endangered.

3. I also feel that clarity is required on how these rights apply to the internet e.g. does assembly apply to groups on the internet?

   Given the importance of the internet in today's world I would argue that a new human right should be created to give the right to access to the internet for all, subject to certain restrictions that protect the right to life, and to ensure usage is in accordance with law and standards necessary in a democratic society.

   This right should place the positive duty on all service providers to prevent harm to other users of the internet. The right should be accompanied by laws to give the courts the right to remove internet access from those who abuse it (in the same way that a persons liberty can be removed by a prison sentence), and ban service providers who do not comply.

4. In January the Prime Minister said that consideration should be given to banning encrypted messaging services such as Whatsapp. I do not believe this is a good idea. Encryption is necessary for financial transactions and for confidentiality reasons. Terrorists can easily circumvent this by simply using code names for people and places e.g. Foxtrot, David's den etc. Public encryption is a bit like locking your front door, it keeps the innocent out but the determined thief can always find a way in.

5. It is illegal for a person to assist another to commit a crime. I find it difficult to accept that no legal action that can be taken against companies who provide services which assist and are therefore used, to plan and execute acts of evil?

   Serious Crime Act 2007 allows for people who assist another to commit an offence to be prosecuted.

   I see no difference in hosting a meeting in my home to hosting conversations on-line. If they are used for criminal intent then the hosting service should fear prosecution.

   I strongly feel that either a new law is required or amendment to existing laws, to make it a criminal offence for companies or organisations to assist those planning and executing crimes. Perhaps the treat of heavy penalties can bring about change.

   If a warrant is issued by a country against a terrorist then the service and content providers should report their usage, or better still prevent them using, their services. Failure to do so would leave them open to prosecution for assisting. Evidence to support a prosecution would be easily obtainable from the suspects internet usage, their online postings and from their email and messages from their mobile phones, and computers.
   I hope these few suggestions will be taken into consideration and I hope your review will be successful.

   February 2015

Media Lawyers Association

Introduction

The Media Lawyers Association ("MLA") is an association of in-house lawyers from newspapers, magazines, book publishers, broadcasters and news agencies. A list of its members is attached at the Annex to this evidence. MLA members publish information not only in the United Kingdom, but also in the European Union and throughout the world. MLA exists to promote and protect freedom of expression and the right of everyone to impart and to receive information, ideas and opinions.

Overview

The MLA welcomes the opportunity to submit evidence to the Investigatory Powers Review. Our evidence addresses those elements of the terms of reference of special relevance to the freedom of expression of our members and of the public.

The review has been launched at a critical time for the protection of the freedom of expression of the media:

- Technological change has resulted in a proliferation of forms in which information associated with journalistic activity is transmitted and stored, and a consequent expansion in the ways in which this can be subject to covert interception.
- The capability and willingness of public bodies, in particular (but not only) law enforcement and security and intelligence agencies, to engage in covert interception has been publicised in a number of high-profile media investigations.
- Specific examples of the use of such methods to obtain material relating to contact between journalists and their sources have come to light, again through investigations conducted by the media.
- Following the ruling of the Court of Justice of the European Union ("CJEU") in the *Digital Rights* case[1] and the quashing of the EU Data Retention Directive[2], Parliament has rushed through the Data Retention and Investigatory Powers Act 2014 to preserve extensive powers of data storage and providing for the very review to which this evidence responds.

In consequence outdated legal regimes enacted in a very different information-gathering context have been overtaken by these, and other, recent developments. It is therefore imperative that fundamental reforms are made to the law regulating investigatory powers

1 *Digital Rights Ireland Ltd and Seitlinger v Minister for Communications, Marine and Natural Resources and Others and Karntner Lendesreigierung and Others and Seitlinger* C-293/12 and C- 594/12

2 Directive 2006/24/EC

used in the context of journalistic activity so as to safeguard the media's role as a public watchdog, which forms one of the cornerstones of a democratic society.

The protection of sources

At the core of our concern about the use of investigatory powers in relation to journal ism is the threat posed to the confidentiality of sources. The fundamental importance of the confidential source to journalistic activity is well-established in English law and in the jurisprudence of the European Court of Human Rights. Among the statements of principle made by the courts are the following:

> "The Court recalls that freedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance (see, as a recent authority, the Jersild v. Denmark judgment of 23 September 1994, Series A no. 298, p. 23, para. 31).
>
> "Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, 18 January 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public- watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest."[3]
>
> "The fact is that information which should be placed in the public domain is frequently made available to the press by individuals who would lack the courage to provide the information if they thought there was a risk of their identity being disclosed. The fact that journalists' sources can be reasonably confident that their identity will not be disclosed makes a significant contribution to the ability of the press to perform their role in society of making information available to the public. It is for this reason that it is well established now that the courts will normally protect journalists' sources from identification."[4]
>
> "88. Given the vital importance to press freedom of the protection of journal istic sources and of information that could lead to their identification any interference

[3] *Goodwin v United Kingdom* (1996) 22 EHRR 123 at [39). This principle has frequently been restated by the European Court of Human Rights: see, for instance, *Weber and Saravia v. Germany (2008) 46 EHRR* SE*47* at 143, *Financial Times Ltd v UK* (2009) 28 BHRC 616 at [70].

[4] *Ashworth v MGN Ltd* [2002] UKHL 29, [2002] 4 All ER 193 at [61].

with the right to protection of such sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake.

89. The Court notes that orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure, and on members of the public, who have an interest in receiving information imparted through anonymous sources (see, *mutatis mutandis, Voskuil v. the Netherlands,* cited above, § 71).

90. First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body. The principle that in cases concerning protection of journalistic sources "the full picture should be before the court" was highlighted in one of the earliest cases of this nature to be considered by the Convention bodies *(British Broadcasting Corporation,* quoted above (see paragraph 54 above)). The requisite review should be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not."[5]

We readily adopt the principles set out above both as to the importance of the safeguarding of confidential sources and to the necessity of robust measures to secure their protection. Their relevance endures at a time when the importance of public interest journal ism has itself been demonstrated by high-profile media investigations into the interception of data by the security services in the UK and overseas. Those same investigations also reveal the fragility of the confidential source in the face of wide-ranging state powers and resources.

Of relevance to the terms of reference of this review, which include the issue of the "safeguards to protect privacy", is the fact that the right to respect for a private life under article 8 ECHR is frequently been held to apply to the protection of confidential sources and other journalistic material.[6]

Interception of communications and access to communications and metadata, and the challenges posed to the practice of journalism

The vulnerability of journalists' digital records and communications to covert interception and access has been vividly illustrated by a number of recent examples, ranging from the large-scale and indiscriminate to the focused and case-specific. These include the collection of communications, traffic and metadata and access to that information:

5 *Sanoma Uitgevers B.V. v The Netherlands* (2010) 30 BHRC 318, Grand Chamber.

6 See *Weber and Saravia v. Germany* (2008) 46 EHRR SE 47 at [78]-[79]; *Telegraaf Media Nederland Landelijke Media B.V. and Others v. The Netherlands* (2012) 34 BHRC 193 at [84]-[88]

- In June 2013 the **Tempora** programme operated by GCHQ was revealed in a number of press reports.[7] By the use of data interceptors connected to fibre optic cables transmitting data in and out of the UK, GCHQ has been able to harvest an immense quantity of data as part of its Mastering the Internet programme for mass communications interception. It has been reported that around 21 Petabytes of data is available for interception daily, equivalent to all the information in all the books in the British Library, in electronic form, 192 times every day. This includes both the **content** of communications and **metadata** about those communications.

- Various other interception programmes undertaken by GCGQ have also been disclosed. These include the **Optic Nerve**[8] and **Global Telecoms Exploitation**[9] programmes and extensive cooperation between the UK and the US NSA, forming part of the latter's **Prism**[10] and **Xkeyscore** intelligence gathering programme. Together these have enabled the security services to gain covert access to an unprecedented quantity of internet, telephone and other telecommunications data, reaching into the private communications of all users of digital media, including journalists. The UK security services rely on the Regulation of Investigatory Powers Act 2000 **("RIPA")** as legal justification for their involvement in these programmes.[11]

- In September and October 2014 it was reported that two police forces had, on two separate occasions, gained covert access to journalists' communication records. with confidential sources. In the Closing Report on **Operation Alice** (September 2014)[12] on the "Plebgate" affair involving Andrew Mitchell MP it was revealed that the telephone records of Tom Newton Dunn, political editor of The Sun, and The Sun's news desk's records, had been seized by the Metropolitan Police in order to trace their communications with a confidential source.[13] No notice had been given to Mr Newton Dunn or to The Sun and the seizure was not judicially authorised. In October 2014 it was revealed that Kent Police had seized the telephone records of a Mail on Sunday journalist, showing communication with a confidential source, as part of its **Operation Solar** investigation conducted in late 2012 in connection with the prosecution of Chris Huhne and Vicky Pryce for perverting the course of justice offences. Again, this seizure had occurred without notice having been given to the

---

[7] See "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian,* 21 June 2013: http://www.thequardian.com/uk/2013/jun/21/qchq-cables-secret-world-communications- nsa

[8] "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ", *The Guardian,* 28 February 2014: http://www .theguardian.com/world/2014/feb/27/qchq-nsa-webcam-images-internet-yahoo

[9] "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian,* 21 June 2013: http://www .theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[10] "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian,* 7 June 2013: http://www. theguardian.com/world/2013/jun/06/us-tech-q iants-nsa-data

[11] GCHQ taps fibre-optic cables for secret access to world's communications", footnote 9 above.

[12] http://content.met.police.uk/cs/Satellite?blobcol=urldata&blobheadername1=Content-Type&blobheadername2=Content-Disposition&blobheadervalue1=application%2Fpdf&blobheadervalue2=inline%3B+filename%30%2260%2F241%2FOperation+Alice+Closing+Report.pdf%22&blobkey=id&blobtable=MungoBlobs&blobwhere=1283788945794&ssbinary=true

[13] "Police seized journalists' phone records in order to out Plebgate whistleblowers", *Press Gazette,* 2 September 2014: http://www.pressgazette.co.uk/police-seized-journalists-phone-records-order-out-plebgate-whistleblowers

journalist and without judicial authorisation. It also came after the police's application to a Judge for a production order for material concerning the confidential source had proven fruitless; and a witness summons application by Huhne's defence team had only resulted in the Mail on Sunday being forced to disclose redacted materials in which the Judge had allowed the identity of the confidential source to be protected.[14]

We derive a number of acute concerns from these examples.

First the capability of law enforcement and security services to intrude upon and to collect electronic communications data is almost unrestricted. In the absence of practical limits on such bodies' ability to intercept such information it is necessary to impose robust legal restrictions.

Second in the course of broad and indiscriminate trawls through such communication data it is inevitable that these bodies will gain access to communications data involving journalists and confidential sources, whether that be the content of such communications or metadata about such communications. Such blanket access to both forms of data has the potential to destroy the confidential relationship between the journalist and the source, with an inevitable adverse impact on the flow of public interest information to the media and then on to the public. To the extent that any such interception is limited to metadata, the concerns remain. Data-mining and link analysis techniques in particular enable collation and synthesising of metadata to powerful effect. Even where such information does not concern contact with a confidential source covert access has the capacity to harm public interest journalism. Communications data disclosing the timing of contact with, or the location of, a known source may disclose critical journalistic information and place that individual at risk.[15] Media investigations of the activities of the police or security services are themselves vulnerable to invasive techniques of information-gathering by such bodies. The value to the security services and law enforcement agencies of metadata is illustrated by the following statements by US and UK public bodies:

> "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content"[16]

> "the distinction between data and content, you can argue, is muddied in the Internet world"[17]

Third it is evident that the police have deliberately used covert techniques in order to violate the confidentiality of the relationship between a journalist and source, circumventing the specific protections set out in section 9 of, and Schedules 1 and 2 to, the Police and Criminal Evidence Act 1984 ("PACE"). Moreover they have shown a propensity to do so in cases which do not come close to involving threats to national security or the most serious forms of criminality. Indeed Operation Alice did result in charges against one police officer, but not against

[14] http://www.thetimes.eo.uk/tto/news/medianews/article4223059.ece

[15] See for instance the facts in *R v Central Criminal Court, ex p Bright* [2001] 2 All ER 244

[16] "The Snowden Leaks and the Public", *New York Review of Books*, 21 November 2013: http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/?pagination=false

[17] Oral Evidence of the Home Office to the Intelligence and Security Committee report into Access to communications data by the intelligence and security Agencies: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf

either of the people who phoned The Sun journalists, although these individuals were later dismissed for gross misconduct following disciplinary action taken by the MPS, as further described in the Closing Report on Operation Alice (see above).[18]

Fourth a wide range of law enforcement powers exist that the police and other authorities have used successfully in order to search, seize and inspect journalists' records on notice and with judicial oversight when such powers are challenged.

Fifth it can fairly be assumed that these cases are the thin end of the wedge. Given the secrecy under which the security services and law enforcement agencies operate, and the lack of effective oversight, it is impossible to estimate the scale of such interception activity and the number of further cases involving or potentially involving journalists' confidential records and communications. However since the cases involving journalistic material referred to above have come to light tangentially in the context of ancillary investigations, and since it is highly unusual for public statements to be made about the use of RIPA against journalists, we suspect that there are in fact many more such cases which have been kept hidden from view.

The failure of existing legal regimes adequately to regulate interception of journalistic material and records

The existing legal controls on these activities are flawed for two overarching reasons. **First** they were in many instances enacted in an earlier age in which the material sought in connection with journalistic activity was likely to be stored in a notebook rather than a server, and the possession of such information lay with the journalist and not with some distant telecommunications company. **Second** even to the extent that such legislation post-dates recent technological developments, they fail adequately to take into account critical factors which threaten the confidentiality of journalistic sources.

Section 9 of, and Schedules 1 and 2 to, PACE set out a detailed regime by which applications for the production of journalistic material are notified to a media organisation to be adjudicated upon by a judge weighing the rights of freedom of expression of journalists against the public interest in investigating crime.[19] It is however evident from the cases listed above that the important protections in PACE are increasingly capable of being circumvented particularly by use of RIPA.

In addition there are a number of other statutory provisions which empower a variety of public bodies to access communications data in certain circumstances, such as the Health and Safety at Work Act 1974, the Criminal Justice Act 1987, the Environmental Protection Act 1990, the Charities Act 1993, the Financial Services and Markets Act 2000 and Social Security Fraud Act 2001. In many instances there is no requirement for prior notification or judicial authorisation for access to communications under these statutes, nor do they fall within the oversight regime for RIPA.

The RIPA regime in particular suffers from a number of flaws which pose a real risk to the confidentiality of journalistic sources. We highlight the following:

---

[18] http://www.thetimes .eo.uk/tto/ news/medianews/article4223059.ece

[19] *R v Crown Court at Lewes ex parte Hill* (1991) 93 Cr App Rep 60; *R (British Sky Broadcasting Ltd) v Central Criminal Court* [2014] AC 885.

- As mentioned above, there is no provision for prior, or post hoe, notification of, or adjudication upon information-gathering programmes which will or may impinge on confidential sources.

- The Secretary of State is vested with extremely broad powers to issue a certificate for the interception of "internal communications" under section 8(1) of RIPA and particularly for the interception of "external communications" under section 8(4) of RIPA 2000. Inadequate legislative safeguards attach to the exercise of this power, again especially in relation to the latter.

- Minimal additional safeguards are contained in The Interception of Communications Code of Practice, which, for interception of internal communications require merely that: "[consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to ... journalistic ... material may be involved" and that "particular consideration" should be given to cases where the "subject" of the interception might reasonably expect a high degree of privacy. By definition any such "consideration" may not take place in respect of interception of external communications where there is no such "subject" identified.

- The Code of Practice for the Acquisition and Disclosure of Communications Data does not mention journalism or Article 10 at all.

- Access to communications data under sections 21 and 22 of RIPA are subject to a much lighter self authorising regime than the already inadequate safeguards for interceptions despite the fact that the information trawled can breach personal privacy and journalistic privilege to the same extent as an interception of content.

- There is a much wider set of purposes for the collection of communications data[20] and it can be collected by a much larger group of public agencies. not just the intelligence and security agencies and the police.[21]

- The oversight regime in relation to RIPA is inadequate:

    - The Codes of Practice are inadequate and the failure to comply is explicitly exempted from any civil or criminal liability.[22]

    - There is no access to the ordinary courts to challenge interceptions or access to communications data under RIPA. Official figures show that of 1469 complaints to the Investigatory Powers Tribunal, which has exclusive

[20] Such as "in the interests of public safety" and for the purpose of "assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department": s 22(2)

[21] Such as the Charity Commission, the Food Standards Agency, HM Revenue and Customs, various Government departments and National Health Service organizations, the Independent Police Complaints Commission and others: see Schedule 2 to the Regulation of Investigatory Powers (Communications Data) Order 2010.

[22] s72(2)A failure on the part of any person to comply with any provision of a code of practice for the time being in force under section 71 shall not of itself render him liable to any criminal or civil proceedings.

jurisdiction over such matters, only 11 were upheld (and 7 of these were joint complaints in just 2 cases).[23]

- The position is not assisted by the role of Interception of Communication Commissioner ("ICC") under RIPA 2000 since the Commissioner has no power to quash a warrant issued under section 8(4), to determine that new arrangements as to interception practices should be made or to determine how deficiencies in existing arrangements ought to be remedied.

- The failure to collect information about the number of occasions when journalistic data (whether content or communications data) is sought or actually accessed prevents the ICC (or others) from properly scrutinising the use of RIPA powers to obtain journalistic material.

- Only a small minority of warrants are reviewed by the Intelligence of Communications or Intelligence Services Commissioners. The House of Commons Home Committee recently expressed its "serious doubts" that these roles should be part-time and expressed concerns that less than 10% of warrants are examined, stating the view that "this figure ought to be at least 50%, if not higher".[24]

Recommendations

Against that background, we consider that reforms to the law are pressing and urgent. Such changes need to address the following considerations:

- The principles of prior notification and prior review by a judge in respect of production order applications under PACE should be extended to other forms of information gathering affecting journalistic activity under RIPA and other legislation save in exceptional cases where this would give rise to a real risk to national security. Such protection must apply whenever a public official has a reasonable belief that a particular interception warrant is likely to result in access to data or information relating to journalistic material, communications or other activity.

- To the extent that any prior notification and adjudication is not possible in any exceptional case, there should be provision for an *ex parte* procedure before a judge and post hoe notification and review to determine the lawfulness of any historic or ongoing exercise.

- The particularly lax regime under RIPA applying to the collection of communications data should be strengthened in recognition of the invasive nature of the information which can be derived from the latter form of data.

- The absence of safeguards particularly in relation to warrants for external communications and insofar as any investigations may impact upon journalistic material or information.

[23] Hansard, HC, 23 April 2009 (column 858W); Hansard, HC Debates, 11 January 2010 (column 701W); Annual Reports of the Investigatory Powers Tribunal (2010-2012) .
[24] House of Commons Home Affairs Committee, *Counter-terrorism* HC 231, 9 May 2014, para 167.

- Effect must be given in the Code of Practice on the Acquisition and Disclosure of Communications Data to the importance of the protection of journalists' sources.

- Careful consideration will need to be given as to whether these changes are implemented by amendment to existing legislation, to the enactment of new legislation and / or to amendment to procedural rules set out in the Criminal and Civil Procedure Rules. Whichever avenue(s) is / are chosen, it will be important to ensure consistency of approach across the various legislative regimes under which interception takes place. Such rules should apply not only to the security services and law enforcement agencies but also to other public bodies which have powers to intercept data.

- More rigorous oversight must be given to the Commissioners over the use of RIPA and other powers in relation to journalistic activity. The Codes of Practice should enshrine special procedures and decision-making processes in cases with a potential impact on journalists' work and should contain specific reference to article 10 ECHR. Statistics should be compiled and published regularly on the use of interception powers in relation to journalistic data and material. The Commissioners should be given a specific mandate to review the use of interception powers in such cases.

October 2014

List of MLA Corporate Members:

1. **Associated Newspapers Limited**, publisher of the Daily Mail, the Mail on Sunday, Metro and related websites.

2. **The British Broadcasting Corporation**, a public service publisher of 8 UK- wide television channels, interactive services, 9 UK-wide radio/audio stations, national and local radio/audio services, bbc.co.uk and the BBC World Service.

3. **British Sky Broadcasting Limited**, a programme maker and broadcaster, responsible for numerous television channels, including Sky News and Sky One.

4. **Channel 5 Broadcasting Limited**, a public service broadcaster of the Channel 5 service and 2 digital channels, interactive services and related websites.

5. **Channel Four Television Corporation**, public service broadcaster ofChannel 4 and three other digital channels, plus new media/interactive services, including websites, video on demand and podcasts.

6. **The Economist Newspaper Limited**, publisher of the Economist magazine and related services.

7. **Express Newspapers**, publisher of the Daily Express, the Sunday Express, the Daily Star, the Daily Star Sunday and related websites.

8. **The Financial Times Limited**, publisher of the Financial Times newspaper, FT.com and a number of business magazines and websites, including Investors Chronicle, Investment Adviser, The Banker and Money Management.

9. **Guardian News & Media Limited**, publisher of the Guardian, the Observer and Guardian Unlimited website.

10. **Independent Print Limited**, publisher of the Independent, the Independent on Sunday, the Evening Standard, i and related websites.

11. **Independent Television News Limited (ITN)**, producer of ITV News, Channel 4 News, Channel 5 News, internet sites and mobile phones.

12. **ITV PLC**, a programme maker and a public service broadcaster of the channels ITV1 (in England and Wales), ITV2, ITV3, ITV4 and CITV, interactive services and related websites.

13. **The National Magazine Company Limited**, publisher of consumer magazines including Cosmopolitan, Good Housekeeping, Harper's Bazaar and Reveal.

14. **News Group Newspapers Limited**, publisher of The Sun and related magazines and websites, and part of NI Group Limited.

15. **The Newspaper Society**, which represents the publishers of over 1200 regional and local newspapers, 1500 websites ,600 ultra local and niche titles, together with 43 radio stations and 2 TV channels .

16. **PPA (The Professional Publishers Association),** which is the trade body for the UK magazine and business media industry. Its 250 members operate in print, online, and face to face, producing more than 2,500 titles and their related brands.

17. **The Press Association,** the national news agency for the UK and the Republic of Ireland.

18. **Telegraph Media Group Limited,** publisher of the Daily Telegraph, Sunday Telegraph and related websites.

19. **Thomson Reuters PLC,** international news agency and information provider.

20. **Times Newspapers Limited,** publisher of The Times and The Sunday Times and related websites, and part of NI Group Limited.

21. **Trinity Mirror PLC (including MGN Limited),** publisher of over 140 local and regional newspapers , 5 national newspapers including the Daily Mirror, Sunday Mirror and The People and over 400 websites .

22. **Which?,** the largest independent consumer body in the UK and publisher of the Which? series of magazines and related websites.

Gavin Millar Q.C

Introduction

1. I represent media organisations and journalists in both the civil and criminal courts. I often act for journalists seeking to identify confidential journalistic sources[1].

2. I have been involved in three cases in which RIPA powers have been used against journalists to identify a confidential journalistic source ("a CJS'").

3. In such cases there may be argument as to whether the RIPA powers have been used compatibly with the presumptive right of the journalist to protect the source (as to which see below). This right derives from the Convention law under ECHR Art 10 but is now well established in our domestic law[2].

4. These cases have attracted much publicity:

    a. In 2008/9 I defended Sally Murrer at Kingston Crown Court on a charge of aiding and abetting misconduct in public office. She was alleged to have received information from a serving police officer, enabling her to write stories for her paper in Milton Keynes. In the course of the investigation Ms Murrer was subjected to intrusive covert surveillance under Pt II of RIPA. The Thames Valley Police placed a probe in Ms Murrer's car and recorded her conversations in the car with the police officer. This was done in order to identify him as her CJS. The Crown was unable to show that the resulting evidence identifying him as her CJS had been obtained in a way that was compatible with the relevant ECHR Art 10 principles and the prosecution was stayed as an abuse of process[3]. There was no evidence that Ms Murrer had ever paid for information from the officer.

    b. In 2012 I represented the Mail on Sunday journalist, David Dillon at Southwark Crown Court. He broke the story about Chris Huhne asking his then wife Vicky Pryce to take speeding points for him. Lawyers acting for Chris Huhne in ***R v Pryce and Huhne*** applied for a witness summons against Mr Dillon requiring production of his emails relating to the original story. The trial judge ordered production of the emails but directed that they be redacted to protect Mr Dillon's CJS. The prosecution gave the disclosed emails to the Kent police. Kent police subsequently obtained David Dillon's phone records which were used, alongside the emails, to identify his CJS. The CJS was a respected freelance journalist. His phone records were also obtained to identify his sources for the story. This was done under RIPA Pt I Ch II. It was said that it was done in discharge of the police obligation to investigate whether Pryce had made up the

[1] See eg ***Mersey Care NHS Trust v Ackroyd (No 2)*** [2008] EMLR, proceedings by a special hospital to obtain my client's source for a story about mistreatment of Ian Brady.
[2] See for example ***Ashworth Hospital Authority v MGN Ltd*** [2002] 1 WLR 2033 paras 38 and 48 indicating that these principles apply in deciding whether a journalist may refuse to identify a CJS under s.10 of the Contempt of Court Act 1981.
[3] See "*Police investigation breached reporter's human rights*", *Media Lawyer,* 28 November 2008.

allegation against Huhne and given it to the press in order to ruin his political career[4].

c. On 1 September 2012 the Metropolitan Police Service published a closing report giving a detailed account of its investigation into the "*plebgate"* affair, Operation Alice. The *Sun* had broken the story about the incident at the Downing Street gates in a front page exclusive on the 21 September 2012. The closing report acknowledged that the investigation had accessed the phone records of Tom Newton Dunn (the Political Editor of the *Sun*) and those for the landline into the newsroom of the *Sun* in order to identify the CJSs for the story. Again this was done under RIPA Pt I Ch II. I am acting for Mr Newton Dunn and the newspaper in complaints about this to the Investigatory Powers Tribunal under RIPA s.65(2)(a)[5].

5. I am concerned that these cases may be the "tip of the iceberg" and that RIPA powers may have been used against journalists in other cases. I suspect this has happened regularly in the recent MPS investigation, Op Elveden, into payments to journalistic sources by journalists at News Group Newspapers.

The problem

The journalist's right

6. This is not the place for a lengthy exposition of the relevant Convention law, but it is important that the reason for the presumptive right is understood:

> *The right of journalists to protect their sources is part of the freedom to "receive and impart information and ideas without interference by public authorities" protected by art.10 of the Convention and serves as one of its important safeguards. It is a cornerstone of freedom of the press, without which sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information to the public may be adversely affected.*

See the decision of the Grand Chamber in ***Sanoma Uitgevers BV v Netherlands*** [2011] EMLR 4 para 72

7. The following aspects of the right are also very important:

a. In any case where the state seeks to identify a CJS it must establish a countervailing public interest of sufficient weight to displace this constant and powerful public interest in the protection of press sources. This has to be done in order to show that the interference with the right is justified as *necessary in a democratic society* under ECHR Art 10.2. See ***Goodwin v UK*** (1996) 22 EHRR 123 at para 39; ***Sanoma*** (above) at para 51.

[4] See eg Fiona Hamilton, *The Times "Police used secret phone records of reporter's source"* 1 October 2014

[5] See eg Lisa O'Carroll, *The Guardian "Sun makes official complaint over police use of RIPA against journalists"*

b. In any case where the state seeks to identify a CJS it must also demonstrate that the evidence required cannot be obtained without having to override the presumptive right of the journalist to protect the CJS. As the dissenting members of the Strasbourg court memorably said in the ***Sanoma*** case when it was before the Chamber

> *...Because of the importance of the principle at stake, the journalist should be the last, rather than the first, means of arriving at evidence required.*

For examples of cases where the state failed to demonstrate this and a violation was found see: ***Roemen and Schmit v Luxembourg*** (App No 51772/99 25.2.03) concerning a police search of the journalist's home; ***Ernst v Belgium*** [2004] 39 EHRR 35 concerning searches of journalists' offices and homes. Again this is required in order to show that the interference with the right is justified as *necessary in a democratic society.*

c. The vital importance of the presumptive right to press freedom means that it *must be attended with legal procedural safeguards commensurate with the importance of the principle at stake*...***Sanoma*** at para 88. This principle falls under the requirement in ECHR Art 10.2 that any interference with the Art 10.1 right is *prescribed by law.* The safeguards required include:

> *...the guarantee of review by a judge or other independent and impartial decision-making body...The requisite review should be carried out by a body separate from the executive and other interested parties, invested with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not...**Sanoma*** at para 90 [emphasis added];

Moreover the determination by *the judge or other independent and impartial body* should be:

> *...governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's sources...**Sanoma*** at para 92

In other words there should be clear law requiring the judge etc to apply the principles at a. and b. above and to prevent the enforced disclosure if the person seeking to displace the presumptive right fails to establish *necessity in a democratic society.*

8. In ***Telegraaf Media Nederland v The Netherlands*** (39315/06; 22.11.12) the Dutch intelligence and security service (the AIVD) was investigating the leaking of secret classified information. Some such information had been leaked to two applicant journalists. Covert surveillance powers were used against the journalists, including powers to intercept and record telecommunications, in order to identify their CJS for the information. The use of the covert surveillance had been authorised by an the

interior minister or an AIVD officer *but in any case without prior review by an independent body with the power to prevent or terminate it...*[6] The case is important because the Court found that the journalists right to protect their CJS was engaged and had been breached because the *legal procedural safeguards* required in the *Sanoma* case were not built into the relevant Dutch law.

RIPA

9. These *safeguards* are not built into RIPA.

10. In none of the three cases referred to above did the relevant parts of the RIPA regime guarantee an independent review of the use of the powers to identify the source, in which the Strasburg principles would be carefully applied to the facts, before the powers were exercised.

11. In ***R v Kearney, Murrer and others*** the intrusive surveillance was authorised by a *senior authorising officer* in the Thames Valley Police, see RIPA s.32. It would have been approved by a Surveillance Commissioner[7]. These provisions, however, make no reference to the right of a journalist to protect a CJS or the need for an overriding public interest. Perhaps unsurprisingly when the authorisation documentation was disclosed in the Crown Court proceedings it made no mention of the fact that purpose of obtaining the recording of the conversations in the car was to identify a CJS.

12. The current Home Office Code of Practice for covert surveillance indicates that extra care is required when it might reasonably be expected that confidential journalistic information will be obtained[8]. But this passage in the guidance, self evidently, does not guarantee the safeguards envisaged in ***Goodwin, Sanoma*** and ***Telegraaf Media.***

13. In ***R v Pryce and Huhne*** and Operation Alice the authorisation notice for obtaining the communication data was provided by a *designated person* in the force concerned under RIPA s.22. It is understood that this was an officer at the rank of Superintendent[9]. It is of particular concern that in the case of Tom Newton Dunn's phone data, this was apparently accessed in the first few weeks of Operation Alice[10] and before he had even been called for interview in the investigation[11].

The solution

14. Those involved in operating the RIPA regime should, of course, understand the relevant Convention law described above and that s.6 of the Human Rights Act 1998 means that they cannot act under RIPA in ways that are incompatible with these journalistic rights. It is trite law that the Convention rights must be respected by public

[6] See at para 100
[7] See RIPA s.36(2)
[8] See at para 4.1
[9] As per Regulation of Investigatory Powers (Communications Data) Order 2010/480, Sch 1.
[10] It started in December 2012 and the source was identified from Mr Newton Dunn's phone data (and arrested) in January 2013.
[11] This did not occur until March 2013. Mr Newton Dunn asserted his right not to identify his source in a prepared statement to the police.

authorities even if the "black letter law" in the domestic statute, looked at in isolation, would appear to sanction a violation.

15. But the government and Parliament must be realistic about this. It is very unlikely that the public authorities in which the RIPA powers are vested will stop using them incompatibly with these rights, simply because the Convention law and HRA s.6 are pointed out to them (perhaps in the Code of Practice). This is so for a number of reasons.

16. The Convention law requires the prior *independent review* procedure to be used. In cases where RIPA does not provide for such a procedure the public authority would have to think well outside of the "box" to find an appropriate procedure elsewhere[12]. Even if such a procedure does exist (for example the approval procedure involving a Surveillance Commissioner under RIPA Pt II) it is asking a lot to expect RIPA users to graft the Convention law onto this procedure simply from their own understanding of that law. It is asking even more to expect them to do it <u>correctly</u> from their own understanding. The Convention law is specialist and requires particular types of material to be laid before the judicial decision taker (eg explaining why there is an overriding public interest and how all other reasonable avenues of investigation have been exhausted). The concept of the overriding public interest is unique and can be difficult to understand and apply properly.

17. My strong preference is that Parliament passes a free-standing "shield" law. This would protect journalists by enacting the relevant Strasburg principles and procedure into our own domestic law. RIPA could amended to divert all cases in which investigating authorities are seeking material tending to identify CJSs into a properly crafted procedure under this legislation. This would require an *inter partes* procedure in all but the most exceptional cases. I appreciate, however, that this form of solution is beyond the scope of this review.

18. I would therefore urge this review to recommend detailed and clear amendments to RIPA, or (even better) a completely updated version of the legislation, designed to achieve this result. I do not think the first solution would be as effective as a free-standing shield law or a new version of the RIPA legislation because amendments can be overlooked. New free-standing laws have more impact. But it is a possible short-term solution.

19. A new section should be introduced into the legislation containing a version of the shield law. It could be headed *Applications for access to information identifying a journalistic source* and adopt the helpful definitions in Recommendation No R (2000) 7 on the right of journalists not to disclose their sources of information promulgated by the Council of Europe's Committee of Ministers viz:

> *a. the term 'journalist' means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication;*

[12] They do exist. If it is known that there is journalistic material on particular premises (perhaps the newsroom of the media outlet) which contains admissible evidence of an offence PACE Sch 1 can be used – leading to a production order application before a circuit judge. In other cases an application for a source disclosure application can be made against the journalist in the High Court.

b. the term 'information' means any statement of fact, opinion or idea in the form of text, sound and/or picture;

c. the term 'source' means any person who provides information to a journalist;

d. the term 'information identifying a source' means, as far as this is likely to lead to the identification of a source:

i. the name and personal data as well as voice and image of a source,

ii. the factual circumstances of acquiring information from a source by a journalist,

iii. the unpublished content of the information provided by a source to a journalist, and

iv. personal data of journalists and their employers related to their

20. The problem of presenting the right information to judicial decision takers in investigation order cases involving confidential journalistic material (including in *ex parte* procedures) has been confronted under Part 6 of the Criminal Procedure Rules. See, just to take one example, for example r.6.7 of the 2014 CrimPR re *Content of application for production order etc* under the Terrorism Act. The suggested amendments to RIPA could be supported by a statutory instrument in similar form covering each type of application for authority under RIPA. No doubt standard forms could be prescribed under the subordinate legislation to ensure that the case for overriding the right to source protection is made properly.

October 2014

National Union of Journalists

The National Union of Journalists (NUJ) is the representative voice for journalists and media workers across the UK and Ireland. The union was founded in 1907 and has 30,000 members. It represents staff and freelances working at home and abroad in the broadcast media, newspapers, news agencies, magazines, books, public relations, communications, online media and photography.

The NUJ has a proud history of supporting journalists and campaigning for the protection of journalistic sources and material. The NUJ's code of conduct has established the main principles of UK and Irish journalism since 1936. The code is part of the rules of the union and members support the code and strive to adhere to its professional principles. The NUJ code of conduct includes the following clause:

A journalist protects the identity of sources who supply information in confidence and material gathered in the course of her/his work.

The existing powers set out in the Regulation of Investigatory Powers Act (RIPA) can be used by a wide range of specified organisations to access journalistic communications and identify journalistic sources. The NUJ believes that these powers have been abused and attempts to obtain journalistic sources and materials should be subjected to independent and judicial oversight.

Following the report in Press Gazette revealing The Sun's political editor Tom Newton Dunn's mobile phone records and call data to the newsdesk were seized by police to expose journalistic sources, NUJ general secretary, Michelle Stanistreet, said:

"Instances like this amount to the outrageous criminalisation of sources who have taken the decision that information they are in receipt of deserves to come to the attention of the public. If whistle-blowers believe that material they pass to journalists can be accessed in this way - without even the journalists and newspaper knowing about it - they will understandably think twice about making that call. The Met’s actions here have been to pursue witch-hunts of their own staff, with clearly not a jot of interest in the wider damage they are causing to public trust in journalism. It is an outrageous abuse of their position which needs urgent addressing."

The NUJ also condemned a further case in which police have misused the RIPA in order to secretly access material from journalists and their sources. The second case involves Kent Police obtaining the phone records of Mail on Sunday news editor David Dillon and freelance journalist Andrew Alderson. Gavin Millar QC has said he was alarmed by the police interventions in both the Huhne and Plebgate cases:

"The crimes being investigated in both these cases are not serious, they are not terrorism and they are not organised crime. There is no justification for using RIPA. It gives an insight into how freely they use this, but how can we have a debate about it unless they are transparent about it."

"They are getting the information without having to do the work and in secret, taking a shortcut without having to go before a judge and justify it and give journalists an opportunity to defend confidentiality of their sources."

Michelle Stanistreet, NUJ general secretary, added: "It is becoming clear that the misuse of RIPA to snoop on journalists is not an isolated example of bad practice in the Met. The police clearly believe they are above the law they are there to uphold. Their utter contempt for journalism and a free press will have a paralysing impact on whistle-blowers who will think twice before ever picking up the phone to a journalist again. Information that deserves to be in the public domain won't see the light of day. The damage to public trust in journalism is immense."

Industry magazine Press Gazette has submitted a range of freedom of information (FOI) requests to the police and more than 25 police forces across the UK have declined to disclose details on whether RIPA has been used to obtain journalists' communications. Nearly half of the police forces asked have rejected the request citing the "risk of undermining national security".

The Interception of Communications Commissioner has now written to all chief constables ordering them to provide full details on the use of RIPA powers to identify journalistic sources. The commissioner has also launched an inquiry. The NUJ welcomes both of these recent developments and we believe it is essential that the review establishes the true facts and those facts and the review findings are both presented in the public domain.
RIPA should not be used to undermine existing protections specified in the Police and Criminal Evidence Act (PACE) as well as the Contempt of Court Act provisions on professional secrecy for journalists, lawyers and others.

We hope that this review will encourage parliament to simplify and clarify the legal framework and we would welcome legislative proposals that provide enhanced protections for confidential sources and materials. Without these protections there is a severe risk to press freedom and the continued abuse of RIPA will detrimentally prevent NUJ members investigating and reporting on local, regional, national and international issues in the public interest.

Further information:
The NUJ code of conduct: http://www.nuj.org.uk/about/nuj-code/

NUJ condemns 'outrageous criminalisation of sources' after police seize phone data
http://www.nuj.org.uk/news/stanistreet-condemns-outrageous-criminalisation-of-sources/

NUJ calls for urgent investigation of RIPA's use to spy on journalists
http://www.nuj.org.uk/news/nuj-calls-for-urgent-investigation-of-ripas-use-to-spy-on/

Gavin Millar QC comments on the Huhne and Plebgate cases:
http://www.theguardian.com/media/2014/oct/06/sun-official-complaint-ripa-journalists-met-police

Press Gazette Save our Sources campaign:
http://www.pressgazette.co.uk/subject/Save%20Our%20Sources

October 2014

The Newspaper Society

The Newspaper Society represents regional media companies which publish around 1100 daily and weekly local newspapers, read by 30 million people a week, with 1700 associated websites attracting 79 million unique users a month, ever developing digital news services and broadcasting interests(www.newspapersoc.org.uk)

The Newspaper Society, Society of Editors and broadcasting companies made representations during the passage of RIPA Bill and thereafter on the necessity for better protection of journalistic sources, as these could be identifiable from information obtained under RIPA powers by the wide range of specified organisations. We suggested that fewer organisations should be permitted to exercise powers under RIPA, the grounds for exercise should be strictly limited and high thresholds imposed, the application and exercise of any powers should be strictly limited to the most senior personnel in all circumstances and all applications for use of such powers should be subjected to judicial scrutiny before any application was granted, especially to protect confidential journalistic sources. We drew attention to the specific safeguards for confidential journalistic sources and material in PACE, the Police Act and the Data Protection Act as well as under the general law. We also supported enhanced transparency and better public oversight of the functioning of the system.

The local media maintained representations to Government at the time of subsequent reviews of RIPA. We felt that the Act and Codes did not provide adequate journalistic safeguards. We were concerned at anecdotal information of attempts to trace the source of leaks of council information by local authorities using RIPA powers of surveillance and access to telephone records. The media also reported the seemingly unjustified use of RIPA powers against individuals by local authorities and others.

Currently, we share the concern of other media organisations on the use of RIPA powers by the police in respect of journalists, including attempts to trace journalistic contacts and sources, seemingly as a convenient means of bypass of the statutory protections contained in other legislation. We re-iterate the need for prior judicial scrutiny and the other restrictions upon application and exercise of such powers. We would therefore support changes to the primary legislation which would provide better protection to confidential journalistic sources and thereby assist media organisations' lawful investigation and report of local, regional, national and international matters. (Conversely, we would obviously be concerned if any changes were proposed that would create new restrictions upon the citizen's and media 's exercise of the right to freedom of expression, as opposed to the state's surveillance of its citizens).

In Europe, the European Newspaper Publishers Association has made similar representations on protection of journalistic sources in respect of relevant prospective EU legislation governing access to communications content, communications data and surveillance.

October 2014

Ofcom

Ofcom's use of communications data and interception powers

Introduction

1. In light of the review of law enforcement authorities' capabilities and powers with regard to communications data and the interception of communications, and of the accompanying regulatory framework, Ofcom sets out:

   a. our powers;
   b. relevant safeguards;
   c. the ways we have exercised our powers; and
   d. the possible consequences of their removal.

   Ofcom welcomes the chance to make these submissions and hopes they are helpful. If it would assist further, we would be glad to discuss them.

2. We have focussed in particular on the use of our information gathering power under section 135 Communications Act 2003 (the "CA03") and our obtaining of communications data under the Regulation of Investigatory Powers Act 2000 ("RIPA"). Other areas we outline are also relevant.

Summary

3. Ofcom has powers to obtain information, which may include communications data,[1] in certain legislation other than RIPA, most particularly the CA03. Those powers are subject to the safeguards in that legislation. In general, they are used to obtain information from, and to regulate the conduct of, corporate entities electing to undertake regulated activities. Though the information obtained may relate to individuals, their identities and conduct are generally incidental to, not the subject of, Ofcom's regulatory activities (the aim of which is to further citizens' and consumers' interests).

4. Ofcom obtains such information and data in order to carry out a range of functions in the CA03 and other legislation. The functions are part of our role as the National Regulatory Authority ("NRA") the UK is required to establish under the European

[1] Within the definition in section 21(4) RIPA and other information that may fall within a broad definition of such data.

common regulatory framework for telecommunications (the "CRF"), and of our role as the UK regulator for postal services, for the electromagnetic spectrum used for wireless telegraphy (the "spectrum") and certain broadcasting matters, and as a concurrent enforcer of competition and consumer law.

5. Some of these functions Ofcom are required by European and/or domestic law to carry out. If we did not have powers to obtain information, including communications data where relevant, we would be unable, or unable without increased difficulty, to carry out some of our functions. This may result in conflict with EU and/or domestic law.

6. Ofcom also exercises powers, including to obtain communications data as a relevant public authority, under RIPA. We obtain such data where necessary for the purposes of investigating and prosecuting criminal offences relating to the spectrum. These may include offences committed by individuals and data obtained may relate to them. Were we unable to obtain such data, this would affect our ability to investigate such offences and fulfil our spectrum management functions and duties.

Background

7. Ofcom is the NRA the UK is required to establish for the purposes of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services ("telecommunications") (commonly known as the "Framework Directive"). We are required under that Directive, and others comprising the European CRF,[2] to carry out a number of functions. We are also the UK's regulatory body in relation to postal services, in relation to the spectrum and in relation to certain broadcasting matters. Concurrently with other bodies, we also have powers to enforce general competition and consumer protection laws.

8. Ofcom was established by the Office of Communications Act 2002. As matters of domestic law, some of which implements the CRF, our main duties, functions and powers are in:

   a. the Communications Act 2003 (the "CA03");
   b. the Postal Services Act 2011 ("PSA11");

[2] Which also includes Directives 2002/19/EC (the "Access Directive"), 2002/20/EC (the "Authorisation Directive"), 2002/22/EC (the "Universal Service Directive") and 2002/58 (the "Privacy Directive").

c. the Wireless Telegraphy Act 2006 ("WTA06");

d. the Competition Act 1998 (the "CA98"); and

e. the Enterprise Act 2002 (the "EA02").

9. Under section 3 CA03, Ofcom's principal duty, in carrying out our functions (see below), is to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition. In carrying out our functions, we are required to secure, a number of things, including the optimal use for wireless telegraphy of the spectrum. Under section 29 Postal Services Act 2011, we are also required to secure the provision of the universal postal service.

10. The functions Ofcom is required to carry out under the European CRF and/or the domestic legislation referred to above include:

a. making and enforcing general conditions of authorisation for telecommunications providers[3] (Articles 1 – 6 and 10 Authorisations Directive, in particular, and sections 45 – 63 and 94 - 104 CA03);

b. market analyses - to determine whether particular providers have significant market power and relevant markets are not effectively competitive, and whether therefore to impose obligations ("SMP conditions") to address those matters (Articles 15 and 16 Framework Directive, as reflected in sections 78 - 91 CA03);

c. resolving disputes between undertakings in connection with regulatory obligations imposed under the CRF and national implementing legislation (Article 19 Framework Directive, as reflected in sections 185 - 191 CA03);

d. investigating compliance with, and enforcement of, provisions relating to persistent misuse of electronic communications networks and services (sections 128 – 130 CA03);

[3] Conditions which apply to operators, in place of a licensing regime, compliance with which authorises an operator to provide telecommunications services.

e. reporting duties, such as that in section 134A CA03 to report to the Secretary of State on the UK's telecommunications infrastructure and to publish that report;

f. making and enforcing universal service and consumer protection conditions for postal operators under sections 42 and 51 PSA11, respectively;

g. to allocate rights to use the spectrum and the issuing of wireless telegraphy licences, investigating complaints of interference to wireless telegraphy and investigating and prosecuting a number of criminal offences relating to the spectrum, under the WTA06;

h. investigating and determining infringements under the CA98; and

i. enforcement under EA02, including in relation to consumer law under Part 8 of that Act.

11. In the exercise of these functions, Ofcom has these powers to gather information that may, depending on the breadth of the definition,[4] include communications data:[5]

a. section 135 CA03 (information required in connection with making and enforcing conditions);

b. section 136 CA03 (information required for statistical purposes);

c. section 191 CA03 (information relating to dispute resolution);

d. section 55 PSA11 (information relating to the carrying out of Ofcom's postal services functions);

e. section 32A WTA06 (information relating to radio spectrum functions);

f. section 26 CA98 (information relating to investigating breaches of competition laws); and

[4] In particular, whether the definition, or any future definition, is broad enough to include aggregated data (e.g. volumes of traffic per communications provider)
[5] As defined in s.21(4) RIPA

g. section 225 EA02 (information relating to consumer law enforcement under Part 8 EA02).

12. Some of these powers (a – c, for example) have their origins in the European CRF. Article 5 of the Framework Directive requires that Member States ensure that undertakings providing telecommunications networks and services provide all the information necessary for NRAs to ensure conformity with the CRF.

13. Ofcom also uses powers in RIPA to obtain and disclose communications data, as well as conducting lawful surveillance under that Act.[6] We are a relevant public authority for the purposes of Chapter II of that Act and may use the powers in respect of communications data where our statutorily designated officers believe it is necessary for the purpose preventing or detecting crime or of preventing disorder. We use those powers in connection with our investigation and prosecution of criminal offences relating to the spectrum.

14. We also have powers relating to the interception of communications in sections 48 and 49 WTA 06.

CA03

General

15. Ofcom's main information gathering power is in section 135 CA03. It enables Ofcom to require from certain persons – principally, telecommunications providers – "all such information" as we consider necessary for the purpose of carrying out our functions under Chapter 1 CA03. Those functions are concerned principally with making and enforcing regulatory conditions, market analyses and investigating persistent misuse of networks and services.[7] The information that may be obtained under this provision includes information likely to be communications data.

16. Section 137 CA03 contains relevant safeguards. Ofcom may not obtain information for the purpose of ascertaining whether a general condition has been breached

---

6 Under Part II of RIPA, in accordance with the provisions of that Part and of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI 2010/521

7 In paragraphs 11(a), (b) and (d) above

unless, for example, we are investigating a complaint to that effect, we have opened an investigation of our own accord or we have reason to suspect a breach. In any event, we are required in any demand for information to describe that information and state the purpose for which we require it. We are prohibited from requiring information except where the making of a demand is "proportionate to the use to which the information is to be put in the carrying out of Ofcom's functions."

17. As to the holding of such information once obtained, Ofcom is a data controller for the purposes of the Data Protection Act 1998 and we are subject to a statutory prohibition on disclosure under section 393 Communications Act 2003, save in accordance with that section.

General conditions and persistent misuse

18. Examples[8] of the circumstances in which we have used section 135 to collect data that is most likely to be communications data are (i) in the making and enforcing of general conditions; and (ii) tracing silent and abandoned telephone calls for the purpose of enforcing the CA03's persistent misuse provisions.

19. As to the first, details of the conditions Ofcom has imposed may be found here: http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/.

20. To take one example, General Condition 11 requires telecommunications providers to levy accurate bills. To enforce this provision, Ofcom would need to obtain information about the extent of communications services provided (and not provided) to individual consumers.

21. We used the power in section 135 in the enforcement action we took against companies in the TalkTalk group for breaching General Condition 11. They had sent bills to over 62,000 customers, for between £1.3 and 1.7 million in total, for services they had not used. Using the power, we were able to obtain from the companies information about the extent to which consumers had used (and not used) relevant services and the bills they received. Our action resulted in us imposing penalties of over £3 million on the companies.

[8] It is probably not possible to predict all circumstances in which Ofcom might consider it necessary to require the provision of information in order to exercise our functions under Chapter 1 CA03.

22. As to the second, section 128 prohibits "persistent misuse" of an electronic communications network or service. This occurs where the effect or likely effect of a person's use of such a network or service is to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety and that use occurs enough times to represent a pattern of behaviour or practice or recklessness as to whether persons suffer annoyance, inconvenience or anxiety.

23. Ofcom has historically focused our enforcement efforts on those committing persistent misuse by making of silent and abandoned calls through the use of automated calling systems. This remains a priority issue for Ofcom.[9]

24. Market research in 2014 suggested that 84% of consumers received unwanted calls on their landline over a four week period; with 61% receiving a silent call and an estimated 14% receiving an abandoned call.[10] Silent and abandoned calls are also the issues that consumers complain about most to Ofcom.[11] In addition, the Minister, Ed Vaizey, has publicly stated that nuisance calls are a serious problem and that "we must do more to combat the menace of silent and unsolicited marketing calls."[12]

25. Many complaints about silent and abandoned calls relate to calls made by persons who have withheld or misrepresented their Calling Line Identification (CLI).[13] In order to trace the true source of such calls, it is often necessary to request information falling within the scope of section 135 from a chain of telecommunications providers, beginning with the telecommunications provider on whose service the call complained about terminated and working backwards from there, using traffic data, towards the originating telecommunications provider. Ofcom also uses the powers in section 135 to obtain from the undertakings making silent and/or abandoned calls, information about the calls they make within any periods under investigation.

---

[9] As set out in Ofcom's Annual Plan 2014/15, it is a major work area, see Figure 3 at http://www.ofcom.org.uk/about/annual-reports-and-plans/annual-plans/annual-plan-2014-15/

[10] http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/nuisance_calls_research/

[11] In 2014, we typically received over 3,000 complaints a month about silent and abandoned calls. For further details, see Figure 2 of Telecoms Complaints Bulletin 26 February 2015, http://stakeholders.ofcom.org.uk/binaries/enforcement/telecoms-complaints-bulletin/February15.pdf

[12] The Minister made these comments during the Westminster Hall debate on nuisance calls 28.02.2013 (http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm130228/halltext/130228h0001.htm)

[13] In its simplest terms, a CLI is a phone number on which an incoming call is made and which may be available to the recipient by dialling 1471 (or some similar service)

26. Ofcom has used its powers in section 135 to enable it to take formal and informal enforcement action in relation to abandoned and silent calls twenty-six times in 2014. The use of these powers enabled Ofcom to take formal enforcement action to protect consumers in four of those cases, for which Ofcom imposed financial penalties totalling £58,000. We also took informal action in 47 cases, and saw complaints stop or fall significantly in relation to 46 of those, while one is ongoing.

27. Our enforcement action in both the above contexts would have been significantly more difficult, perhaps not possible, had we not had the section 135 powers to obtain communications data and other relevant information from the relevant telecommunications providers. Proving infringements of rules on accurate consumer billing depend on information about the extent of individual customer's use of communications services. Investigating persistent misuse cases depends on our ability to identify those making silent and abandoned calls. That is unlikely to be possible without the ability to obtain from telecommunications providers information about the use of their networks as well as, from those undertakings making the calls, records of their volume.

28. In these contexts, the information Ofcom is able to obtain is often from entities who have chosen to undertake regulated activities and relates to specific aspects of those activities. The information is obtained and used to protect consumers' interests. To the extent it involves data about individual consumers, their identities and conduct are incidental to, rather than under, investigation.

Other uses of section 135

29. The above are only examples of the use of our information gathering power in section 135. It is likely that some of Ofcom's other regulatory duties and functions would require us to obtain communications data. It is difficult exhaustively to set out which and to what extent. We cannot easily predict exactly what issues may arise, leading us to seek to impose different or amended regulatory conditions in future. Some of our duties and powers are relatively untested and may in future involve the obtaining of communications data.

30. Even so, we can provide relevant indications. For example, Ofcom has used our powers in section 135 CA03 to gather information on internet traffic speeds at the level of individual premises, as part of meeting our duty to prepare reports on infrastructure under section 134A CA03.

31. There are also cases where, should communications data be given a broad definition, so as to include information such as aggregated data about the use of networks and services ("volumes data"), Ofcom uses section 135 to obtain such data. A number of these are matters which Ofcom is required by the European CRF and/or UK legislation to undertake. If we did not have the ability to obtain this data, there is a risk of Ofcom and/or the UK coming into conflict with our obligations (as summarised above).

32. For instance, Ofcom is, as noted above, required under the Framework Directive and CA03 to undertake market analyses and, where we find markets are not effectively competitive, to impose SMP conditions on undertakings having significant market power. These analyses go to promoting effective competition in markets that are worth many millions, sometimes billions, of pounds. They typically involve Ofcom using section 135 to obtain volumes data. Were we unable to do so, competition in the relevant markets may be less effective, to consumers' detriments in relation to price, choice, quality and innovation, as well as risking conflict with Ofcom's and the UK's legal obligations.

Other powers

33. Ofcom may also obtain information, that may include communications data and/or volumes date, under other powers.

34. One example is in section 191 CA03, which gives Ofcom the power to require parties to disputes about relevant regulatory conditions or parties holding information relevant to such disputes, to give us "all such information" as we require to decide whether to determine a dispute and how to do so.

35. Depending on the regulatory conditions involved, such disputes may involve a need for Ofcom to obtain communications data and/or volumes data. Without a power to obtain such data, Ofcom may be unable to determine disputes, in conflict with the relevant provisions of the European CRF and/or CA03.

36. Another important example is Ofcom's information gathering powers under PSA11. In October 2011, as a result of PSA11, Ofcom assumed responsibility for regulating postal services from Postcomm, the previous postal regulator. In his 2010 report Richard Hooper stated that under any new regulatory framework for postal services "the regulator must have enhanced statutory information gathering powers."[14]

37. Section 55 (and Schedule 8) PSA11 were intended to fulfil the objective Richard Hooper set out. Section 55 (and Schedule 8) is similar to section 135 CA03. It enables Ofcom to require certain persons – principally postal operators, but also others who may have relevant information – to provide us with "all such information" we consider necessary for the purpose of carrying out any of our functions on postal services. It contains similar safeguards about the purposes for which information may be obtained and the form and proportionality of any demand for information (see Schedule 8 paragraphs 1 – 4).

38. Ofcom uses these powers to collect a range of essential information in relation to its functions. Some of this may fall within the current definition of communications data and some under any broader definition including volumes data.

39. For example, Ofcom uses Section 55 to collect information on actual and projected volumes, revenues and costs of different postal products (letters, parcels, etc.) from different postal operators. This is necessary for Ofcom to fulfil its primary duty to secure the provision of a financially sustainable and efficient universal postal service. We also need on occasion to collect information relating to business plans and intentions.

40. Such information is necessary for the imposition and enforcement of designated universal service provider conditions (including, for example, price controls), universal service provider access conditions, universal service accounting conditions, essential conditions (relating in particular to mail integrity), general access conditions and consumer protection conditions. These are set under sections 36, 38, 39, 42, 49, 50 and 51 PSA11, respectively. We may also need to obtain communications and/or volumes data to monitor Royal Mail's compliance with quality of service requirements.

[14] *Saving the Royal Mail's universal postal service in the digital age*, p.8. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31808/10-1143-saving- royal-mail-universal-postal-service.pdf

41. Relevant to these powers and safeguards is Article 22a of Directive 97/67/EC on common rules for the development of the internal market of Community postal services and the improvement of quality of service. This provides that Member States shall ensure that postal service providers provide all the financial information and information concerning the provision of the universal service necessary for NRAs to ensure conformity with the Directive.

42. A further relevant power is in section 225 EA02. Under Part 8 of this Act Ofcom has concurrent jurisdiction with other enforcement bodies to bring proceedings in relation to breaches of consumer protection legislation, where such breaches harm consumers' collective interests. Section 225 provides for a related information gathering power.

43. Of particular relevance is our concurrent jurisdiction with the Information Commissioner's Office to enforce against breaches of certain provisions of the Privacy and Electronic Communications (EC Directive) Regulations 2003. These include those provisions prohibiting the making of unsolicited marketing calls to persons who have registered with the Telephone Preference Service that they do not wish to receive such calls.

44. Section 225 EA02 provides Ofcom with the power to obtain information about calls made in defiance of this prohibition. That will involve information likely to include communications and/or volumes data, without which Ofcom may be unable to take action to protect consumers (whose identities and conduct would be incidental to, rather than the subject of, the action).

45. It is possible we may seek to collect communications and/or volumes data using the power in section 32A WTA06. For example, to help us determine how the electro-magnetic spectrum should be optimally used. Likewise, using the power in section 26 CA98. For example, to investigate whether a dominant undertaking has engaged in a margin squeeze in respect of the pricing of relevant products or services.

RIPA

46. Ofcom is a relevant public authority for the purposes of Chapter II RIPA, by virtue of which we may obtain and disclose communications data. We may, however, collect

such data only for the purpose of "preventing or detecting crime or of preventing disorder."

47. We do so principally for the purposes of investigating and prosecuting criminal offences relating to wireless telegraphy under the WTA06. These include offences set out in Chapter IV of that Act, such as unlicensed broadcasting[15] and related offences. These are triable either way and, on conviction on indictment, a person may be imprisoned for up to two years and/or subject to a fine (unlimited).

48. We also do so for the purposes of investigating and prosecuting offences under the Radio Equipment and Telecommunications Terminal Equipment Regulations 2000 (the "R&TTE Regulations") and the Electromagnetic Compatibility Regulations 2006 (the "EMC Regulations").[16] These regulate the placing on the market and putting into service of telecommunications and other electrical apparatus liable to cause harmful interference to uses of the spectrum (such as services used for public and State security, defence, and including aeronautical uses and mobile phone networks).

49. Ofcom has a duty to enforce the R&TTE and EMC Regulations.[17] They provide for offences liable to summary conviction and to punishment in some cases by up to three months' imprisonment and/or a level 5 fine, and in others to a level 5 fine.

50. Ofcom is specified for the purposes of section 25(1) in Chapter II RIPA as a relevant public authority, by virtue of Article 3(3) and Schedule 2 of the

---

[15] pirate radio, for example

[16] SI 2000/730 and SI 2006/3418, respectively.

[17] Both say Ofcom has a, "…. duty…. to enforce these Regulations …. insofar as action taken to enforce a regulation relates to the protection and management of the radio spectrum" (Schedule 9, Part 1, paragraph 1 and regulation 37, respectively

Regulation of Investigatory Powers (Communications Data) Order 2010.[18] Only certain individuals - those holding the position of "Senior Associate responsible for spectrum investigation technology support" - are prescribed to exercise relevant powers.

51. Under Article 5(1) of that Order, the individuals within Ofcom who may grant an authorisation or give a notice relating to the exercise of RIPA powers to obtain communications data may only do so where they believe it is necessary for the purpose specified in section 22 (2)(b) RIPA. That is, for the purpose of "preventing or detecting crime or of preventing disorder." They may not grant an authorisation or give a notice unless they believe that obtaining the data in question by the conduct authorized or required is proportionate to what is sought to be achieved by so obtaining the data (section 22(5)).

52. Between 1 January 2012 and 31 December 2014, Ofcom conducted 2753 criminal investigations under the witness telegraphy-related legislation described above. In respect of those investigations, Ofcom exercised its powers under RIPA in respect of communications data as follows:

a. applications for authority approved by Designated Person: 52 (21 in 2014, 20 in 2013 and 11 in 2012);

b. authorisations issued by Designated Person: 81[19] (36 (2014), 29 (2013) and 16 (2012)); and

c. notices issued to Communications Service Providers: 40 (22 (2014), 10 (2013) and 8 (2012)).

53. The communications data which was the subject of these authorisations and notices covered a number of different types. These included telephone numbers, email addresses, handset PINs, social media account details, IP addresses and other website information and SIM-card details.

[18] SI 2010/480
[19] The number of authorisations in (b) exceeds the number of applications in (a) because each application could include acquisition of more than one type of data.

54. Most of Ofcom's applications for authorisations and notices to obtain communications data arise from the seizure of mobile phone handsets during searches under judicial warrant[20] of unlicensed broadcast stations and/or premises from which equipment under investigation under the R&TTE or EMC Regulations is sold, or found in the possession of persons arrested for such crimes. Communications data such as subscriber and call details provide evidence of association with unlicensed broadcast stations and other individuals involved in their operation and/or of steps taken to place equipment on the market in possible breach of the R&TTE or EMC Regulations.

55. Ofcom uses the powers to obtain communications data under RIPA as part of a range of evidence gathering powers and processes. These include test purchases and exercising powers of search and seizure, including under warrant, provided for by the WTA06 and the R&TTE and EMC Regulations, making broadcast recordings, and interviewing suspects under caution. We seek to use the powers under RIPA where we are unable to identify individuals involved in the suspected criminal activity and it is therefore necessary to obtain communications data to help identify them.

56. Without the relevant powers in the relevant circumstances, Ofcom would be unable, or able only with significantly increased difficulty, to identify relevant individuals and potential criminal activity. This would be liable to cause an increased risk of harmful interference to important kinds of spectrum use, which may include use for air traffic control, use by the emergency services, use by licensed broadcasters and listeners and by mobile telephone network providers and their consumers. If Ofcom is unable to enforce the R&TTE and/or EMC Regulations, we risk coming into conflict with our duty to do so.

Interception under sections 48 and 49 WTA06

57. Ofcom also has powers under sections 48 and 49 WTA06 to use wireless telegraphy apparatus to obtain information as to the contents, sender or addressee of messages[21] of which we are not an intended recipient. We may only do so under the authority of Ofcom officers designated for that purpose in accordance with sections 48 and 49.

[20] Powers relating to warrants, search and seizure are in sections 97 and 99 WTA06, paragraphs 8 and 9 of Part I of Schedule 9 R&TTE Regulations and regulations 39 and 40 EMC Regulation.

[21] whether sent by wireless telegraphy or not

58. Under Regulation 3 of the Wireless Telegraphy (Interception and Disclosure of Messages) (Designation) Regulations 2003,[22] Ofcom's Operations Director and Head of Field Operations are designated to give the relevant authority. Section 49 WTA06 contains relevant safeguards.

59. In particular, the effect of sections 49(2) - (5) is that a designated person may only give authority, which must be in writing and may be general or specific,[23] for the purposes of section 48 and 49 where:

a. it is necessary on grounds such as national security, preventing or detecting crime and public safety; or

b. it is necessary for purposes connected with Ofcom's duties and functions under the WTA06; and, in either case,

c. the conduct authorised is proportionate to what it seeks to achieve (having taken into account whether the outcome could reasonably be achieved by other means).

Where the authorised conduct would otherwise fall within RIPA, it may only be authorised where (b) and (c) apply. The effect is to take that conduct outside RIPA, but subject to the safeguards in sections 48 and 49 WTA06.

60. Ofcom's designated person has issued relevant authority to our field officers (spectrum engineers and criminal investigations officers). They use this authority on a day-to-day basis to identify sources of interference to the spectrum. Without that authority Ofcom would be unable, or unable without severe restriction, to investigate and manage such interference at the time it occurs. This could have severe adverse effects on spectrum uses affecting many aspects of everyday life (mobile telephone networks, broadcasting, emergency services and air-traffic control, for example).

March 2015

[22] SI 2003/3104
[23] see section 49(8) WTA06

Sir David Omand GCB
Visiting Professor, Department of War Studies King's College London

(a) **What balance should be struck between the individual right to privacy and the collective right to security?**

1. The invocation of a balance in relation to collective 'rights', although useful shorthand, is problematic since it implies the more of one for society must logically imply the less of the other. That is not necessarily the case with security, a condition that provides the fundamental basis upon which other rights can be more easily secured. A State that is suffering insecurity will be badly placed to deliver the protection of other rights, including privacy. I define **Security** as *a state of confidence* that the major risks facing the public at home and when abroad are being managed satisfactorily - so that people can make the best of their lives, and live freely (that is, with their essential democratic freedoms and rights protected) and with confidence (the public uses crowded spaces, business has confidence to invest, international travel and trade is possible, and markets are stable). Around the world we can see all too readily countries where this condition fails and where basic human rights suffer as a consequence.

2. The challenge of supporting national security has changed the nature of the demands for secret intelligence, for example in uncovering the rapidly growing threats to cyber security and thus to our economic prosperity. There are many insistent demands from law enforcement for pre-emptive intelligence to arrest or to disrupt terrorist plots and to protect the public by preventing threats crystalising. Intelligence is needed to support military operations, often in near-real time.

3. Often the demand is for actionable intelligence about people - non-State actors - the dictators, terrorists, insurgents, hackers, cyber- and narco-criminal gangs, and people traffickers, concerning their identities, associations, location, movements, financing and intentions, not to mention the Russian paramilitaries in Ukraine and ISIL jihadists in Iraq and Syria. Of course, there are still demands for intelligence on some traditional States and their intentions – but even there the communications of interest are likely to be on mobile devices or carried on virtual private networks on the internet.

4. Intelligence has significant public value since it helps to improve the quality of decision-making, whether by police officers, military commanders or policy makers, by reducing ignorance about the threats that face us. Intelligence agencies must therefore be close to their customers and know what information would be relevant to those decisions, would add value and the timescale for key decisions. Obstinately, there remains vital information that the enemies of our free society - the dictators, terrorists, insurgents, cyber- and narco-criminal gangs and others - do their best to prevent us knowing. It is the purpose of *secret* intelligence to overcome the will of these others and to supply to our police officers, military commanders, and policymakers at least an insight into the threats posed.

5. The inevitable consequences of seeking secret intelligence are the moral hazards attached to the methods necessary to overcome the will of the other and the secrecy that must surround sources and methods so that our adversaries are not forewarned of how to avoid our attentions. An example of the moral hazard is the risk that there will be collateral invasion of the privacy of those not under investigation and whose communications are warranted to be intercepted. This results in a classic Type1/Type2 error problem. If the cursor is set at negligible risk then it will not be feasible to gather the required intelligence. If the cursor is set too high then there will be unacceptable levels of intrusion. Where the cursor is set is a political choice, for the Secretary of State to judge what is proportionate in relation to the level of harm that the intelligence operation is intended to reduce. No risk is not an option.

6. What is important is that our public has that confidence in the way that the UK government goes about taking action to manage the major risks that affect us, including in this context the extent to which the State has to intrude upon both the privacy of any individual and that of fellow citizens. That overall level of confidence will have several components.

a. One component is confidence that there is a sound and up to date legal framework within which the executive and judicial authorities must act (and the confidence that such law can be readily accessed and understood if needed – there can be no secret law[1]).

b. A second component is sufficient confidence that those taking risk management decisions (Ministers, senior officials and police officers) share the values of a free and democratic society and that they apply ethical principles in their work. A suggested set of such principles for interception is annexed to this note[2].

c. A third component is confidence in the adequacy of the checks and balances on the exercise of the State's coercive powers to reduce the likelihood of abuse of power and illegal behavior through the work of the Committee and the Commissioners and through the internal processes of warranting and control within the intelligence agencies and their parent Departments.

d. A fourth component is confidence that the major threat assessments that justify both the maintenance of intelligence capabilities – and the relevant *jus ad intelligentiam* – and their application to specific cases – and *jus in intelligentio* – have been objectively and fairly evaluated.

7. I draw the Review's attention therefore to a recent UK opinion poll[3] that bears on the subject that shows clearly that the British public has such confidence in the system. Although there is certainly a minority that is concerned over intrusions into privacy, the poll shows a large majority of adults in the UK (71%) think that the government should "prioritise reducing the threat posed by terrorists and serious criminals even if this erodes peoples' right to privacy". The same poll shows around 2/3 of adults think that British intelligence agencies should be allowed to access and store the internet communications of criminals or terrorists and around 2/3 also back them

[1] As appears to have been the case with 'warrantless interception' in the US authorized by the US President under the Patriot Act
[2] See David Omand, *Securing the State,* London, Hurst, 2010, chapter 10.
[3]TNS-BMRB, Polling 23-27 January 2014, www.tns-bmrb.co.uk/news-and-events/britons -give-safeguarding-security-a-higher-priority-than-protecting-privacy, accessed 4 Feb 2014.

in carrying out this activity by monitoring the communications of the public at large. Indeed, most people expected such surveillance to be in place.

8. I conclude that the public as a whole approves of the 'balance' currently being struck.

How does this differ for internet communications when compared to other forms of surveillance, such as closed circuit television cameras?

9. There are at present very different laws regulating these two forms of surveillance, for historical reasons. As technology advances, for example by enabling sophisticated facial and pattern recognition software to be applied to the visual images captured digitally by advanced high-definition CCTV, then its use will become more often a case of directed surveillance as already defined under Part II of RIPA2000 and as already applies to some CCTV use. It may be that the Review will recommend changes in Part II, although the development of the technology may make it wise to wait a few years before legislation is drafted. In the meantime it may be that the Codes of Practice can take the strain, for example by raising the level at which such directed surveillance may be authorized. But the distinction in RIPA2000 between Part I – interception, broadly speaking – and Part II – directed surveillance - remains in my view a valid one from the point of view of the legal construction of that legislation and the complex interaction with other relevant legislation.

To what extent might it be necessary and proportionate to monitor and collect innocent communications in order to find those which might threaten our security?

10. 'Monitoring' requires sentient (human) examination of the material and must be distinguished from 'collection' (or 'access', in many ways a more appropriate term). A category error has crept into much of the recent public debate over the material stolen by Edward Snowden and passed to journalists of not distinguishing bulk access to the internet – which the UK certainly does have for example through transatlantic cables[4]– and so-called 'mass surveillance' which it does not conduct, and about which Sir Anthony May's annual report is reassuring. I hope that the Review will be able to produce and publish an authoritative account of this distinction.

11. It is important that the public be reassured that we are not being monitored as a population and being subject to mass surveillance, and be reminded (as Sir Anthony May has emphasized) that it would be unlawful for the intelligence agencies to conduct this. Mass surveillance is about pervasive observation or monitoring of the entire population or a substantial sector of it. Observation implies observers, human beings who are examining the thoughts and actions of the population.

12. GCHQ, in pursuit of its foreign intelligence mission (the Review will be very aware of the need to assess risks posed by returning British jihadists who have been fighting in Syria – the current counter-terrorist alert state is 'Severe') must in my view continue to have bulk access to large volumes of traffic on the internet. The necessity for this stems from the nature of the modern packet switched networks, the exponential growth of internet traffic and its global distribution.

[4] As revealed in 1968 by Chapman Pincher in the Daily Express

13. The warranted bulk access will be needed to find the wanted traffic of the small number of legitimate targets, as set out in the certificates required to accompany RIPA2000 8(4) warrants – what has been described as finding the needles in a vast set of internet haystacks. Internal control procedures inside GCHQ must continue to ensure that only that authorized traffic and data is examined by its analysts. More could be done in the Code of Practice to describe how in general terms the system works, following the lead taken by Sir Anthony May in his 2013 Annual Report. The use of the term 'mass surveillance' by commentators with its echoes of the Stasi observing and controlling by fear the East German population is simply journalistic sleight of hand to damn the US National Security Agency and GCHQ by association.

14. The volumes of internet traffic, and the way that communications are compressed, bundled and routed (and increasingly encrypted) will inevitably make real-time access impossible from many large and important bearers. The issue might be addressed by buffering and temporarily storing the digital streams which could then be subject to computer examination and application of selectors and discriminators[5] to pull out for human analysis the wanted communications data and, where warranted, the content of the communications. For how long such material needs to be stored will need to be kept under review as the technologies change. It should be the minimum necessary to achieve the approved purposes and no more. In my view, it would be a mistaken policy to follow the US example and to seek to retain large quantities of data for very long periods before selection and analysis 'just in case' future intelligence requirements change.

How does the intrusion differ between data (the fact that a call took place between two numbers) as opposed to content (what was said in the call)?

15. It has always been possible to derive intelligence from the fact of a telephone call having taken place. The calling number, called number, length of call and their location (originally through the location of the telephone exchange; today through the location of cell towers) has provided generations of police officers for example the ability to locate missing persons, test alibies and pursue investigations without the need to intrude upon the content of conversations. Where the data indicates that content may be necessary to the investigation and its access would be a proportionate response in relation to the seriousness of the matter being investigated then a case for a warrant can be considered. But that is only in a minority of the cases. So the existence of the distinction, enshrined in RIPA2000, is itself a major protection from privacy intrusion.

16. The same arguments, *pari passu*, applies to the work of the intelligence and security agencies in pursuit of their legal purposes[6]. The Guardian for example has not explained to its readers the important difference between the strict UK legal definition of 'communications data'[7] and the much looser concept of 'meta-data' used especially in the United States to refer to data use by powerful modern tools when data mining from internet and social media activity.

[5] Such as the Internet Protocol (IP) address of a suspect's mobile device

[6] E.g. Intelligence Services Act 1994: In the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; in the interests of the economic well-being of the United Kingdom; and in support of the prevention or detection of serious crime.

[7] RIPA s.21(6)

17. It is the case that with many internet forms of communication (such as social media) it is possible technically to derive much more intelligence about a suspect than could be gleaned from studying the traditional communications of previous eras. Such 'meta-data' as it is called is widely culled by the private sector and sold on for the purposes of marketing of products and services. The internet user implicitly consents to this intrusion as part of the small print conditions for using the service concerned and has in some cases the option of privacy settings to prevent such use of their personal information. Naturally, I would expect the intelligence and security agencies to adopt such techniques to help achieve their approved purposes – but to apply them to cases only once they have the necessary legal authority under RIPA2000 Chapter 1. The communications data that can for example be authorized by senior police officers under RIPA2000 Chapter 2 is subject to the strict (and old fashioned) definition in s.21(6).

18. Channel 4 News, for example, got themselves tangled up[8] over the Dishfire database that NSA has, of information culled they say from millions of text messages a day. Were NSA to allow GCHQ analysts to use a database containing such data, as the Review will be well aware, those analysts could only access it in a way compliant with the narrow UK definition in RIPA2000; if they want to access any content held by the US on a database such as Dishfire they would have to have the relevant Secretary of State warrant.

19. My understanding is that a GCHQ analyst is authorized to treat as communications data only material specifically meeting the legal tests set out in RIPA2000 e.g. the IP address of the suspect machine or email address of the user, when and from where the communication originated, and the server identity being accessed[9]. Thus the analyst can find out under the rules for communications data that the suspect accessed Google - but not the questions asked; that the suspect accessed Amazon but not what was purchased.

20. In shorthand, this is referred to as internet communications data up to the first slash as in www.google.com/ .... Everything beyond that is content for which the analyst requires a warrant from a Secretary of State. A similar position arises with emails - the email address to which an email is sent is considered communications data but not what is in the title of the message and nor the message itself.

Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted.

21. I was PUS in the Home Office when the RIPA Bill was developed and I can assure the Review that great care was taken by Parliamentary Draftsmen to make the definitions of Part 1 covering interception technology neutral. The argument that because RIPA 2000 predated Facebook and social media and so-called 'scraping' technologies the Act must inevitably be inadequate is bogus. The growth and directions of internet use were apparent by 2000. Any case for change in the provisions must be argued on the merits of the need for the change.

22. Indeed, those who argue for change should be careful over what they wish for. I referred earlier in this note to the important difference between the strict UK legal definition of

[8] Channel 4 News, 17 January 2014.
[9] RIPA Section 2(9)d

'communications data' and the much looser concept of 'meta-data'. It would in my view be a mistake – since it would weaken protection against unnecessary intrusion – to change the RIPA2000 definitions by modernizing them to align with modern meta-data techniques. I am not aware of any pressure from the authorities to expand this to cover additional forms of meta-data and would oppose such a change.

Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

23. The care that was taken to make the legal definitions in RIPA2000 technology neutral is in part responsible for the complication of the wording of the Act. That places greater importance on the Codes of Conduct written in accessible plain English for the exercise of the powers under RIPA2000, codes which are publicly available on the .gov website. These Codes are presented to Parliament and are an essential – but alas much neglected – source of reassurance about how RIPA2000 operates in the internet age, and for example how legally privileged material and journalistic material must be handled if inadvertently intercepted and the key role of the Interception Commissioner.

24. I suggest that the Review give particular attention to the Codes and where they could be usefully expanded and updated to give Parliamentarians, the media and the interested public a much clearer view of the purposes for which interception is authorized (with examples), how modern interception has to work in a packet switched internet age, the part GCHQ as a foreign intelligence agency plays in supporting some domestic investigations, and the treatment of meta-data in relation to the RIPA2000 communications data definitions. In my view, more could have been done over the last few years of rapid technological change to explain these matters to the public, and the Codes of Practice could provide an authoritative vehicle for filling this gap (they are subject to positive assent by Parliament).

25. A further media confusion that could be cleared up in this way is over the American legal distinction between US and non-US persons. The US Constitution protects the privacy of US persons anywhere in the world – the main issue that motivated Snowden - but does not offer the same protection to non US citizens. UK law on the other hand does not discriminate between British citizens and others over authorizing intrusive investigative powers. As the Review knows RIPA2000 makes the geographical distinction between the communication of persons in the British Isles - where the Home Secretary is the Secretary of State accountable to Parliament for inter- and persons overseas or communicating overseas - where it is the Foreign Secretary who is accountable. The UK position is in my view actually more compatible with the European human rights tradition as incorporated in the UK Human Rights Act in terms of privacy rights being universal.

October 2014

Annex

There must be sufficient cause to justify the acquisition of intelligence capabilities. Any tendency for the secret world to encroach into areas unjustified by the scale of potential harm to national interests has to be checked. British legislation already does this satisfactorily in terms of the limited purposes for which intelligence can be collected.

There must be integrity of motive. No hidden agendas: the integrity of the whole system throughout the intelligence process must be assured, from collection to analysis and presentation.

The methods used must be proportionate. Their likely impact must be proportionate to the harm that is sought to prevent, for example by using only the minimum intrusion necessary into the private affairs of others.

There must be right and lawful authority. There must be the right level of sign-off on sensitive operations, with accountability up a recognised chain of command to permit effective oversight, both Parliamentary and independent judicial assessment of compliance with the law.

There must be a reasonable prospect of success. All intelligence operations need careful risk management, and before approval is given there has to be consideration of the likelihood of unintended consequences and the impact if the operation were to be exposed or otherwise go wrong and harm innocent parties.

Recourse to secret intelligence must be a last resort. The necessity for using intrusive methods must be demonstrable. There should be no reasonable alternative way of acquiring the information by non-secret methods.

Open Rights Group

Introduction

Our surveillance regime must be necessary and proportionate. It must also achieve democratic and public legitimacy. We accept that the executive is likely to find it difficult to achieve an appropriate balance in the face of security concerns, as evidenced by the Prime Minister's recent remark that "I am simply not prepared to be a prime minister who has to address the people after a terrorist incident and explain that I could have done more to prevent it". This means it is vital to place limits on the executive's powers.

There are large-scale trends that make this a thorny issue. SIGINT measures were originally designed to take advantage of the relative ease of interception of electronic communications, however, most of these communications were not individual to individual, nor purely domestic. This included communications such as radio, phone and satellite communications, which were easier to intercept than letters sent by post. SIGINT measures have always taken advantage of this. Today, communications methods in general have expanded and the digital world makes surveillance even easier. The expansion of this approach means we have slipped into a mass surveillance model without a democratic debate regarding the consequences.

The UK is working very closely with the US and regards this relationship as a crucial factor for the purposes of national security and maintaining international influence. UK and US agencies collaborate extremely closely, sharing data and techniques, even to the point of direct funding from the US to the UK. Whilst this makes it more difficult for the government to consider reining in data collection, it is not a justification for that collection. Accepting this approach without debate is democratically weak and places our relationship with a foreign power ahead of accountability to the British people. It is also questionable whether it is beneficial for the UK to be viewed internationally as the eavesdropper for the US.

The surveillance issue directly affects the UK's reputation abroad and our ability to assert human rights norms in less democratic parts of the world. It may serve to undermine our influence on the world stage, in particular with our European partners and in the eyes of European citizens. Whilst the US has been forced to grapple with the issue and has at least held a thorough democratic debate, the same cannot be said of the UK.

It is essential that this review is wide-ranging and comprehensive.

1. Current and future threats, capability requirements and the challenges of current and future technologies;

Challenges of current and future technologies

In this section we explain how recent technological changes bring into question three critical arguments made by those who defend the surveillance status quo:

1. There is a fundamental distinction between less intrusive communications data/metadata and communications content.

2. There is no mass surveillance because “no human reads, looks or listens” to all the collected information.

3. Bulk collection is needed in order to find the “needle in a haystack”.

New sources of data

There is a qualitative difference between the data available now, in the digital age, and the data available in the pre-Internet days. Data generated now is of a markedly different *type* to phone records and other traditional types of communications data. Taken together, the availability and the quality of new data sources make the distinction between communications data and content unclear in terms of intrusiveness.

A record of a phone call from before the internet tells an investigator who called whom, when, and where. Even this 'traditional' communications data is intrusive and was deemed to require regulation. But digital communications data is even more intrusive. Although only the fact that a particular website was accessed, and not the specific page, is recorded, such information can still speak volumes. The fact that someone repeatedly contacted Narcotics Anonymous, or Gaydar, or a political website goes some way toward indicating significant aspects of their identity or personality. 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 – certainly a far more detailed picture than phone records or even the *content* of a phone conversation could offer.

The Article 29 Working Party of European data protection commissioners argued that the now **void** 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.”

The EU Privacy and Electronic Communications Directive, implemented in the UK as the

Privacy and Electronic Communications Regulations[i], sets strict restrictions on what communications companies can do with traffic and location data.

Metadata allows for intrusion that is comparable to the direct surveillance of an individual. The work of several human operatives to follow the movements and contacts of a target can be achieved just by looking at someone's digital footprints. This was illustrated by German MP Malte Spitz, who made six months of mobile phone records available to journalists. These, combined with the data from social media and publicly available sources, provide an incredibly detailed picture of Mr Spitz's activities[ii].

However, the newer kinds of 'communications data' that the intelligence agencies can access in their wholesale internet surveillance programmes can paint a far more intimate picture of our lives. Researchers have confirmed that simple endorsements in **social media** reveal likely political opinions, sexual preferences, lifestyle preferences, social circles, habits and patterns of behaviour. This is just based on clicking activities, without the person's providing any details[iii].

Intelligence agencies and security services very soon will have access to a wealth of data from cars and home appliances such as thermostats and fridges. The so-called **Internet of Things** will eventually see most electronic gear connected to the Internet in order to exchange all forms of data with users, manufacturers and third parties. A review of interception needs to address not just the handling of such data by agencies, but the threat of sabotage of domestic appliances. There is widespread evidence that GCHQ engages in actively hacking computer systems, including those belonging to innocent third parties.

A particularly concerning development is the emergence of **wearable** technologies and health **sensors** which can track not just minute movements but also a broad range of physiological information.

The Article 29 Working Party has raised concerns about the potential inferences derived from such data:

"Apparently insignificant data originally collected through a device (e.g. the accelerometer and the gyroscope of a smartphone) can then be used to infer other information with a totally different meaning (e.g. the individual's driving habits). This possibility to derive inferences from such "raw" information must be combined with the classical risks analysed in relation to sensor fusion, a phenomenon which is well-known in computer science.[iv]"

The amalgamation - or "triangulation" - of databases is a well known problem for privacy, and allows the re-identification of previously anonymous data[v]. Current discussion about the intrusiveness of mass surveillance generally do not take this into account.

From the Snowden documents we know that the NSA maintains huge amounts of collected communications data in a complex system of storage and retrieval. Specialised databases keep content and metadata for every type of communication imaginable. For example, the database MARINA[vi] is used to store internet metadata of millions of web users for a year, allowing for "pattern of life" analysis. FASCIA[vii] collects 5 billion mobile phone data records from around the world, including location[viii] that allows the tracking of millions of individuals and groups, through the CO[ix]-TRAVELER programme.[x] Several systems collect phone calls, videos, VOIP calls, etc. The UK's role in some of these programmes is unclear.

David Omand has made the case that the legal definition in RIPA of xi"communications data" is a much smaller subset of the general metadata from internet use and social media. According to Omand, most such metadata would probably be classified as "content" in the UK, and receive stronger legal protections, as it is more intrusive.

We do not find the definition of communications data in RIPA s21 narrow at all. But we think that the blurring of the lines between metadata and content that David Omand refers to should be an important consideration for the review. The Home Office acknowledged in their evidence to the Intelligence and Security Committee (ISC): "the distinction between data and content, you can argue, is muddied in the Internet world[xii]".

The same report by the ISC also shows that GCHQ makes few requests under RIPA for "communications data" as such. Because their activities are externally focused, it seems that they mainly collect metadata as collateral of their interception warrants for content and associated communications data. This will involve much larger amounts of metadata than a notice on a communications provider. The handling of the metadata by GCHQ before any safeguards are applied should be clarified, particularly in relation to automated machine processing.

Privacy International has an open case at the Investigatory Powers Tribunal, which has shed unprecedented light on the legalities of bulk data collection and mass surveillance.[xiii] The government refused to officially confirm the existence of any programmes, but confirmed suspicions[xiv] that authorisation for any systems, if they ever existed, would take place under Section 8(4) of the Regulation of Investigatory Powers Act (RIPA). This section allows the Secretary of State to sign general warrants for whole classes of external communications - sent or received outside the British Islands – and associated communications data.

In order to justify the collection of online data, the agencies class many internet activities carried out by people in the UK - such as Google searches and Facebook messages - as external communications. This was explained in the witness statement from the head of the Office of

Security and Counterterrorism, Charles Farr,[xv]. The Code of Practice for interception makes clear that even if communications leave the country, as long as both ends are in the UK they do not fall under Section 8(4). However, the security agencies argue that if Peter sends a Facebook message to John, both of whom are in London, this is in fact two sets of messages to and from Facebook, which is abroad and thus external. xvi

It is increasingly untenable to sustain these legacy distinctions regarding intrusiveness along such rigid lines: communications content and communications data, communications data and metadata, and external and internal communication. We need a more dynamic and contextual framework for analysing the intrusiveness of surveillance.

Machine processing

Advances in machine learning and artificial intelligence should make us question the current focus on human activities in surveillance legislation and policy. The often-heard argument that there is no mass surveillance if “nobody reads, looks or listens” to the collected information is out of touch with the capacities of modern digital systems.

Sir Iain Lobban, head of GCHQ from 2008 until January 2014, made a big point about this, when he stressed in evidence to Parliament[xvii] that operatives do not access all the collected data:

"We do not spend our time listening to the telephone calls or reading the e-mails of the majority, the vast majority that would not be proportionate. It would not be legal. We do not do it."

David Omand has also argued along similar lines:

“Furthermore, the media fall into the category error that has crept into much of the recent public debate of not distinguishing bulk access by computers to the internet – which the US and UK certainly do have – and so- called ‘mass surveillance’, which they do not conduct. Mass surveillance implies observers, human beings who are monitoring the population.”

In legal terms, these arguments refer to the section 16 of RIPA[xviii], which sets out the specific safeguards for the further processing of materials collected in bulk collection programs. But this section only refers to how “intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant”. Unfortunately RIPA is not clear on the safeguards for computer processing of the data.

The developments in machine learning since the time when RIPA was created make the lack of strong regulations on machine processing more risky. Any review must consider the detailed

regulation of computer processing of all types of data or content directly obtained or intercepted.

For example, in recent years facial recognition has finally reached maturity. Despite the lack of publicly available information on their operational effectiveness in the field [xix] these systems are being rolled into production.

There are documents showing that GCHQ engages in computerised facial recognition. GCHQ has tapped into the private webcam communications of innocent Yahoo! subscribers, collecting millions of pictures including substantial amounts of explicitly sexual materials.[xx] The programme, apparently unknown to Yahoo!, targeted 1.8 million unwitting users in a six-month period without any form of minimisation or filtering. In its own documents, the agency explains it did this as an experiment to improve facial recognition, and that the metadata and images were also fed into key NSA databases and the XKEYSCORE search engine.

The need to read emails is reduced by technology that can process text content. This is not even top secret. The NSA makes available, under its technology transfer program, several tools to process natural language texts. These do not require a human operative to actually read them[xxi]. The NSA also licenses technologies for handling voice, including speaker recognition. It is to be expected that GCHQ uses these or similar technologies:

"NSA's acoustic technologies include methods for identification, extraction, and analysis of voice and voice signals. Additional technologies include foreign language voice recognition, duplicate voice identification, and methods of measuring voice enhancement.[xxii]"

Facial recognition and text analysis are stable technologies. The most advanced machine learning technologies are capable not just of recognising a specific individual's face, but of learning to classify faces based on attributes such as hair style or expression [xxiii]. Computer systems from Google can even learn new concepts from pictures and videos, such as figuring out what is a *cat*[xxiv].

These development have far-reaching implications for regulating surveillance. Claims that intrusion only takes place when humans are involved in "reading, listening to, or looking at" are hard to sustain, give the information that can be gleaned by computers alone.

Predictive analytics

In contrast to the US, there is no official confirmation of the existence of mass surveillance programmes in the UK. But officials from GCHQ have defended the practice of bulk collection of data, and all parties have agreed to reintroduce wholesale retention of communications data into UK law. The argument in both cases is that it is acceptable to collect and process vast

amounts of data on the whole population because the agencies only target a minority of troublemakers.

This is the “needle in the haystack” argument that has been repeated many times. We contend that this is a misleading argument, because modern profiling systems do not operate with such clear categories. Instead everyone is analysed and subjected to dynamic risk analysis that at any time could make an innocent citizen a suspect: a needle.

The needle in a haystack line was used by an unnamed GCHQ source in declarations to the Guardian at the time of the first Snowden disclosures:xxv

"Essentially, we have a process that allows us to select a small number of needles in a haystack. We are not looking at every piece of straw. There are certain triggers that allow you to discard or not examine a lot of data so you are just looking at needles. If you had the impression we are reading millions of emails, we are not."

Sir Iain Lobban, head of GCHQ from 2008 until January 2014, used the metaphor of the “needle in the haystack” extensively in his appearance in Parliament in November 2013.xxvi

These arguments are meant to reassure us that if we have nothing to hide, we have nothing to fear, because intelligence agencies only look for the *needles.* But this argument is disingenuous because it is based on the false premise that needles are a distinct, separate category from the hay. Contemporary predictive analytics systems used for the security profiling of the population operate under a very different logic that does not have such fixed categories.

The details of systems used by GCHQ remain mostly secret, but scholars such as Louise Amoore have been studying profiling systems in other areas of national security such as borders and detention orders. These systems are based on data mining techniques that have been developed in commercial applications at casinos, in fraud detection, etc.xxvii

The mechanics of security profiling are in play in border controls. Here we could imagine actual lists of dangerous people who will be prevented from entering the country or possibly taking a plane. The Home Office describes the National Border Targeting Centre (NBTC) – responsible for border profiling – in these simple terms:

“More than 100 million passenger movements in and out of the UK were checked against UK Border Agency and police watch lists last year. (Home Office press release)xxviii”

But this does not fully reflect the way the newer border controls operate for everyone. There are watch lists with named individuals, which raises serious questions about accountability. However, the computers at NBTC perform more complex real-time risk assessments of airline passengers, where those with a substantial risk score are flagged when they cross the border. This score is not fixed, making you *hay*, but will be recalculated at each trip. Buying a ticket in cash, or having taken a previous trip to a troublesome country, when combined with other factors, can trigger an alert. But this does not imply certainty that the traveller is a *needle*; it simply means that the algorithm has assigned that person a higher risk score and that the operative may want to check.

This brings us to another important aspect of security profiling that makes it harder to distinguish the needles from the hay: each individual element of the risk analysis may be completely lawful, but the triggered response when these elements are combined by the ranking algorithms may not be. This has been evidenced in the creation of deportation orders for individuals who are deemed too dangerous to be allowed to remain, but where there is not enough admissible evidence to press charges in an open court. In the words of a defence lawyer at one such case at the Special Immigration Appeals Commission:

“Neither we nor our clients were given the 'ingredients' of the mosaic – we were only given conclusions, expressed in the form 'we assess that X has been involved in attack planning.' This is the way it operates, piecing together fragments which in themselves are innocent..xxix

The argument of the identifiable needle in the haystack is also undermined by the probability models developed around the War on Terror. There is a wealth of research on how the unimaginable events of 911 fundamentally changed security risk calculations. The basic premise is that the mere xxx**possibility** of a high impact event is enough to trigger a response. The UK National Security Strategy encapsulates this way of thinking:

“(...) this strategy must allow the Government to make choices about the risks we face. Of course, in an age of uncertainty the unexpected will happen...xxxi“

The fixed categories of innocent and suspect become more blurred when we are not trying to establish probabilities but simply possibilities. For example, in the period around Christmas 2012-13 NBTC issued 4,900 alerts to border agencies, but these carried out 237 arrests . xxxii

In the sophisticated mass surveillance programs of the NSA and GCHQ, such as XKEYSCORE, all internet users are treated like airplane passengers. After the data on known identifiable targets – the needles – is pulled, the rest of the data is still analysed. The haystack is not discarded but used to build databases for emerging risk calculations. For example, the lawful and innocent use of encryption in emails or searches of the TOR website will be recorded and

potentially linked to other future activities later on to build a higher risk score.xxxiii

These developments make bulk collection an intrusive infringement on the human rights of many innocent internet users, not just the few *needles*. In the context of air travel or border control there could be an argument that this intrusion is necessary for the safety of the flight, and limited to that context. But mass surveillance programs are permanently tracking what we do online.

The risks of profiling outside of national security are acknowledged in the proposed draft European Data Protection Regulation (not applicable to national security), which aims to give EU citizens a general right

"not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour"

In summary, the argument that if you have nothing to hide, you have nothing to fear because mass surveillance is actually targeted at a small minority does not hold. Everyone who is subjected to surveillance is permanently examined and analysed for risks.

A review of surveillance must engage critically with this and the other main arguments made by proponents of the status quo, which unfortunately are too often taken at face value.

2. The safeguards to protect privacy;

Surveillance is only legitimate when it is targeted, authorised by a warrant, having been judged by a court to be necessary and proportionate. The right to privacy is not only a fundamental human right but it is also essential to the protection of other rights. In particular, the right of people to communicate in private is a key part of their right to speak freely.

Privacy and freedom of expression also have collective benefits and create social good. One person having broad protections for their speech enriches public debate. Such protections ensure people can challenge widely held ideas and that those in power cannot easily stifle criticism. Similarly, privacy rights bring collective goods. The right to privacy is a foundation for many things that a tolerant, liberal democracy depends upon. For example, having some control over who is party to a person’s political conversations helps to support free thinking and debate.

Article 8(1) ECHR states that 'everyone has the right to respect for his private and family life, his home and his correspondence'. The courts have since held 'correspondence' to include phone calls, emails and Internet use[xxxiv]. Article 8(2) sets out the circumstances in which interferences with the right are permitted. An interference must be in accordance with the law; necessary in a democratic society; and serve one of the defined interests (such as national security). An interference will be considered “necessary in a democratic society” if it answers a “pressing social need”; and it is proportionate to the legitimate aim pursued and if the reasons justifying it are “relevant and sufficient”.[xxxv]

A central issue is that surveillance should be targeted rather than mass.

In *Kennedy v UK*[xxxvi] the Court considered RIPA in the context of internal communications. It found that those provisions did not violate Article 8. However the Court made clear that its reasoning was limited to internal communications. Central to its conclusion was that,

“in internal communications cases, the warrant itself must clearly specify, either by name of by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered. Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA.“ (at [160], emphasis added).

The ECtHR’s judgment in *Liberty v UK*[xxxvii] points strongly to the external communications provisions of RIPA being incompatible with Article 8. In that case, the court considered the analogous provisions relating to external communications[xxxviii] that applied before RIPA came into effect. Those provisions were in materially identical terms to RIPA and in two respects were more protective.

The ECtHR held that the provisions of Interception of Communications Act 1985 relating to interception of external communications were insufficient to comply with Article 8. The Court accepted that the power to intercept external communications contained in section 3(2) (now RIPA s.8(4)) “allowed the executive an extremely broad discretion” (at §§64-65). Warrants could cover “very broad classes” of communication such as all submarine cables having one terminal in the UK carrying external communications to Europe (or the United States). Thus any person who sent or received any form of telecommunication outside the British Isles could have such communication intercepted. The discretion granted was, therefore, “virtually unfettered”. Precisely the same reasoning applies to the interception of external communications under section 8(4) of RIPA.

We call for the following safeguards to protect privacy and ensure human rights compliance:

a) Judicial warrants

All intrusive, directed and targeted surveillance (including interception, access to communications data and the use of covert human intelligence sources) should be authorised by a serving judge. This will allow the judiciary to perform its proper function of ensuring the rule of law is upheld. At present this power is exercised by a Secretary of State (in the case of the interception of communications), or a senior member of the relevant agency (in the case of authorisations for access to communications data, directed surveillance and the use of covert human intelligence sources). There is only qualified provision for judicial authorisation under RIPA in respect of the authorisation of intrusive surveillance by police (but, notably, not the intelligence services), in respect of requests for encryption keys under Part 3 of RIPA, and for local authorities seeking access to communications data.

Any arrangement which allows the executive to self-authorise the use of surveillance powers is, in our view, entirely unacceptable. It is the proper constitutional function of the independent judiciary to act as a check on the use of state power. Judges are best suited to applying legal tests to ensure that surveillance is necessary and proportionate pursuant to Article 8(2) of the ECHR. The involvement of judges improves public trust and confidence in the system of surveillance. David Bickford, the former Legal Director of MI5 and MI6, recently told a European Parliament inquiry that judicial authorisation is needed, stating: ‘not only does this procedure reduce the risk or perception of collusion but, by removing the executive from these decisions, limits the room for accusations of political interference, and properly complies with the obligations of the state under ECHR’.

English law has long recognised the need for a judicial warrant before a person’s home can be searched by the police. There is no longer any meaningful distinction between the quantity and nature of personal information that can be collected during a premises search and that collected via the targeted surveillance practices permitted under RIPA.

The introduction of prior judicial authorisation for all surveillance powers is, in our view, long overdue. The European Court of Human Rights recognised the desirability of prior judicial authorisation for surveillance in Klass v Germany in 1978, saying: ‘The rule of law implies, inter alia, that an interference by the executive authorities with an individual’s rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and proper procedure.’ In its recent decision in Digital Rights Ireland, the Grand Chamber of the CJEU similarly expressed the view that retention of communications data should be subject to ‘prior review carried out by a court or by an independent administrative body’. Under no

circumstances could a Secretary of State or a senior member of the same public body be described as meeting these necessary requirements of independence and impartiality.

A new surveillance law should contain a clear set of requirements that must be satisfied before any surveillance can be authorised by a judge, namely the requirements of Article 8 ECHR (set out below under recommendations for a new legislative framework).

In conducting the assessment of whether a particular instance of surveillance is justified, a judge would consider whether it pursues a specified
legitimate aim, whether it is necessary to achieve that aim and whether it is proportionate i.e. the least intrusive way of achieving the aim identified.
New surveillance legislation must mandate judicial authorisation of all surveillance decisions including the interception of communications and access to communications data. Access should also be limited to a smaller number of public bodies and restricted to data that is necessary for the prevention, detection or prosecution of serious crimes.

b) Interception of communications should be targeted, not mass

In order to protect privacy we must stop the mass interception of communications without suspicion. Suspicion-less, mass surveillance is disproportionate. A new legislative framework should:

1. Expunge the internal/external distinction from the threshold criteria for the institution of communications surveillance measures. Save in exceptional circumstances that are both clearly and narrowly defined, all interception warrants should be targeted at a specific individual or premises. In any event, interception warrants should never be so broad as to allow for indiscriminate surveillance.

2. Raise the threshold applied to the interception of communications. Interception should only occur after it is established, on case by case basis, that
(i) the surveillance is necessary for a legitimate aim, and the surveillance is proportionate to that aim;
(ii) other less intrusive investigative techniques have been exhausted;
(iii) information accessed will be confined to that reasonably relevant to the investigation, with excess information promptly destroyed or returned; and
(iv) information is only accessible by the specified authority and used for the authorised purpose.

3. The procedural safeguards applied to intercepted material should not differ based on an individual's nationality, residence, location or choice of communications service provider.

Intercepted material provided to the UK by foreign intelligence agencies should also be subject to the same protections and safeguards as material intercepted by the UK. The UK should seek and receive assurances that British standards will be complied with when providing intercepted material to foreign partners (see below for further discussion on international cooperation).

c) Retention of communications data should be targeted, not mass

The collection of and access to communications data should only be available on the same terms as the interception of communications. It has become clear that the existing distinction drawn between content and communications data is untenable.

The law has traditionally treated access to communications data as a less serious interference with the right to privacy than the interception of the content of private communications. The interception of communications under Part 1 of RIPA requires a warrant from the Secretary of State whereas access to communications data under Part 2 requires only authorisation by a senior member of the public body involved.

However, devices now routinely track individuals' location along with the details of the websites visited and the people with whom individuals email, text or chat. Our phones no longer store just our phone numbers but also personal information about our family members, our financial status, our medical history, our political affiliation and religious beliefs. By analysing communications data alone, analysts can build up complex pictures of individual lives: where people go, whom they meet, what kinds of services they use and the types of websites they visit without reading a single email or listening to a single phone call.

In June 2014, the US Supreme Court acknowledged this radical change when Chief Justice Roberts noted that 'today many of the more than 90 per cent of American adults who own cell phones keep on their person a digital record of nearly every aspect of their digital lives'.[xxxix] In recent months, ex-NSA General Counsel Stewart Baker has said 'metadata [communications data] absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.' [xl] General Michael Hayden, former director of the NSA and the CIA, called Baker's comment 'absolutely correct,' and offered a different perspective on the value that the NSA places on metadata, asserting, 'We kill people based on metadata.'[xli]

RIPA and DRIPA must be overhauled to end mass data retention. The CJEU reached a similar

conclusion in April 2014, when it found that the EU Data Retention Directive (which provided for EU States to mandate the retention of communications data for 6-24 months), violated the rights to privacy and data protection under the EU Charter of Fundamental Rights. The CJEU described the regime as a 'wide-ranging and particularly serious interference with those fundamental rights... without... being... limited to what is strictly necessary'.[xlii] In particular, the blanket retention of communications data was found to be disproportionate,[xliii] as was the lack of an independent judicial or administrative judicial body to make decisions regarding access to the data.[xliv]

The Government's rushed through new 'emergency' legislation in July 2014 with only three days of debate in Parliament. The Data Retention and Investigatory Powers Act (DRIPA) does nothing to address the fundamental problems of blanket data retention and the lack of independent authorisation of access. Instead, section 1 of DRIPA puts blanket data retention on a statutory footing, with only minor changes from the previous legislation. In our view it breaches the right to privacy on the same grounds as the previous regime.

Retention must be targeted, justified and subject to judicial authorisation. For example, retention of a person's data would be justified where the person is under suspicion or there is reason to believe it would assist the investigation of serious crime. Retention in a particular geographical area or time period may also be justified.[xlv] DRIPA must be replaced with legislation that prohibits blanket retention and takes account of the other findings of the CJEU.

In addition, there should be exceptions for communications that are subject to an obligation of "professional secrecy".[xlvi] Retention periods should be limited to what is strictly necessary and tailored to different data types and circumstances.[xlvii] The government has introduced regulations[xlviii] that provide for 12 months as a maximum retention period, but these still allow all communications data to be retained for the maximum period without any tailoring. As discussed above, access to the data should be independently and judicially authorised and limited to fewer organisations and circumstances.[xlix] Safeguards should be applied to the stored data.[l]

d) The purposes of surveillance should be clarified

Mass surveillance is undertaken in the pursuit of broad aims and objectives such as 'national security' and 'serious crime', governed by laws that have been rendered out of date by changes in technology and weak democratic oversight. It is for Parliament, rather than the executive, to decide the circumstances and conditions under which law enforcement and intelligence services may have recourse to surveillance powers. New legislation therefore should set out, with much greater clarity than is currently the case, the types of situations in which we may be subject to

surveillance.

We note, for instance, that nowhere in RIPA is there any requirement that an investigating body should have reasonable suspicion that a person is involved in serious crime as a trigger for the use of surveillance powers. Sections 5(3) and 22(2) of RIPA, for instance, set out only the purposes for which surveillance may lawfully be used. The identification of a legitimate aim is a necessary but not a sufficient condition for the use of surveillance powers. In particular, we see no reason why the requirement of 'necessity' should not be brought more closely in line with the requirements of the criminal law in this area. This would assist in narrowing what are otherwise broad definitions, e.g. 'national security' or the statutory definition of 'terrorism' under section 1 of the Terrorism Act 2000.

e) There must be a right to redress

The Investigatory Powers Tribunal (IPT) allows for secret procedures, offers little (if any) rationale for its decisions and is not subject to appeal in any court of law.

All legal challenges against the use of surveillance powers granted under RIPA are currently heard by the IPT (under Part IV of RIPA). The procedure operated by the IPT is seriously flawed and unfair to complainants. The IPT is under no duty to hold oral hearings. Even if it chooses to hold a hearing, all of its proceedings, including oral hearings, can be conducted in private. The IPT cannot disclose to a complainant the fact that a closed hearing is taking place, the identity of any witness or any information provided at the hearing, unless those attending the hearing, the witness, or the provider of the information consent.

There is no provision for special advocates to represent the interests of the excluded party at any closed hearing (although the tribunal does on occasions appoint counsel to the tribunal). If the IPT finds against a complainant it cannot give reasons for its decision; this ‘neither confirm, nor deny’ policy leaves individuals unclear whether they were subject to lawful surveillance that was authorised under RIPA or not subject to surveillance at all. If the tribunal upholds a complaint it is only required to provide the complainant with a summary of its determination. It is telling that in the first decade of the tribunal's operation, it upheld only ten complaints, five of which came from members of the same family and concerned surveillance by a local authority that the authority admitted.[li]

There must be provision for appealing a decision of the IPT. The presumption must be that the IPT will hold public hearings in open court, save where the tribunal is satisfied that private or closed proceedings are necessary in the interests of justice. Any party excluded from closed proceedings should be entitled to sufficient disclosure so that they can bring an effective challenge to any surveillance decision or provide instructions to any special advocate.

f) International co-operation arrangements should be subject to scrutiny

International arrangements governing the collection and sharing of the products of surveillance must be made public and subject to the oversight of Parliament and the courts. This requirement should be set out in legislation and should allow individuals to foresee when they are likely to be subject to surveillance. This would not require disclosure of any detailed information concerning operations, techniques or capabilities but rather the publication and enactment of a legal framework that will apply to the transfer of individuals' sensitive data, including that of UK residents.

At present it appears that the UK government may have frequently circumvented domestic legal procedures by relying on secret arrangements with its intelligence allies that enable the collection, storage and sharing of significant and substantial amounts of information about individuals' online communications. Intelligence arrangements must be subject to public, legislative and judicial scrutiny. Where the government obtains intelligence from its foreign allies, it must meet the same standards that are applicable to its own surveillance activities and should require that its allies meet similar standards. As noted above, it remains unclear that any legal framework governs GCHQ's receipt of data from the NSA.

Greater transparency is also required in respect of GCHQ and the NSA's joint operations. The information exchanged appears to be extensive, with pooled resources making it hard to tell who has access to the information and who is ultimately accountable. For example, the joint programme MUSCULAR[lii] taps into the internal cables of Google and Yahoo and is run by GCHQ from the UK. It is unclear how information relating to British citizens is protected during processing by the NSA, as privacy protections under US law are limited to US persons. We know that that the NSA pays GCHQ substantial amounts of money for its support, some £100m in the three years running to 2013.[liii] It is possible that besides funding GCHQ's core capabilities the payments also provide some form of legal and information ownership structure for certain joint activities.

In addition, to ensure privacy rights are protected:

- It is necessary to improve oversight by Parliament and the Commissioners (please see question 6 below);
- The government should publish aggregate information on the number of surveillance authorisation requests approved and rejected in order to increase transparency (please see question 5 below).

- The Government should cease breaking encryption standards and undermining Internet security. Such activity should be explicitly prohibited by legislation.

3. The implications for the legal framework of the changing global nature of technology;

A major weakness in the current framework governing interception of communications is the lack of any corresponding restriction on the intelligence services obtaining intercepted material from other countries, even where the communications in question belong to people within the UK. Despite the extremely close cooperation between GCHQ and the NSA, for example, it is striking that there are no statutory restrictions to prevent the NSA from supplying GCHQ with access to all the private communications it has obtained from its own extensive surveillance programmes on non-US nationals.

4. The case for amending or replacing the legislation;

The existing legislation has proved inadequate to protect the public from infringements of the rights to privacy and freedom of expression. We need a new, comprehensive piece of legislation governing surveillance powers. The disclosures associated with Edward Snowden have revealed that: surveillance is not covered by adequate legislation; the existing laws ostensibly designed to cover surveillance are badly outdated; and there are serious weaknesses in processes designed to provide oversight and accountability.

In our view this review should cover not only the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Retention and Regulatory Powers Act 2014, but also all legislation on which the Government has acknowledged it relies, including:

a) the Security Service Act 1989;

b) the Intelligence Services Act 1994; and

c) the Counter-Terrorism Act 2008.[liv]

Although RIPA was originally intended to bring UK law in line with the requirements of the ECHR as incorporated by the Human Rights Act 1998 (HRA), it is clear that its poor drafting and opaque structure have not prevented a massive expansion in the scope of surveillance powers in the last 15 years. It was also drafted before the rapid and unprecedented change in communications technology.

The law in this area simply has not kept pace with the scale of technological change. The

protections that Parliament intended to enshrine in RIPA no longer offer adequate oversight of the technical capabilities of Britain's security services. As a result, gaps and weaknesses in the framework have been exploited to enable the collection of our private communications on a previously unimaginable scale. The intelligence agencies, left virtually unconstrained and unsupervised by outdated legislative frameworks have unilaterally expanded the scope of their activities and the extent of their capabilities.
The revelations regarding the TEMPORA programme have shown that according to the Government's interpretation, RIPA allows mass and indiscriminate interception of the communications (both content and metadata) of almost the entire UK population.

RIPA has enabled our intelligence services to exploit antiquated statutory definitions, changes in communications technology, and without adequate oversight. The law is now being applied in secret, so that we, the public can no longer know what is being done in our name. The so-called safeguards that RIPA contains have proved woefully inadequate to ensure proper accountability and they have failed to ensure that surveillance powers have been exercised proportionately.

New legislation must be put in place to ensure that surveillance conducted by law enforcement and intelligence agencies is only carried out where it is strictly necessary and proportionate. It must contain statutory definitions that reflect modern circumstances, not the now antiquated framework of the past. It must contain effective and rigorous oversight mechanisms to ensure that the intelligence services are not able to expand their powers in secret. Most of all, the law must be changed in order to ensure that our fundamental rights and the rule of law are protected, rather than undermined.

It is a fundamental principle of the rule of law in any democracy that people must know how the law is being applied. When public officials exercise intrusive powers in secret, it is all the more important that the law sets out clearly the circumstances and conditions in which those powers can lawfully be exercised. It has become clear that our surveillance laws are damaging our privacy, our freedom of speech and our very democracy. It is time for significant and urgent change to re-establish the basic tenets of the rule of law, namely transparency, accountability and protection for the fundamental rights of every person.

The collection of information through surveillance programmes is in itself an infringement of privacy. It is not only the access to and use of that data that needs to be subject to controls and safeguards, and it is not only through 'access' to data that the activity becomes 'surveillance'. For instance, there are inevitable vulnerabilities to large stores of data, with the risk of malign or accidental access, disclosure or loss, and a danger of function creep.

The introduction of DRIPA demonstrated that for some time the UK security services had been

interpreting RIPA on a very broad basis, which would have continued had the service providers not insisted on warrants and RIPA notices having a solid legal basis. It appears that the intelligence services' existing capability did not have a proper legal basis, which was why the DRIPA provisions relating to RIPA were required. We believe that unless there are checks and balances in the system then the intelligence services will do what they can get away with, regardless of what the law actually says. Mere "oversight" amounting to a rubber-stamp is not sufficient.

We have particular concerns about sections of RIPA including but not limited to the following:

Section 8(4)

In particular, the Snowden revelations regarding the scope of GCHQ surveillance under TEMPORA have highlighted the use of warrants for the interception of so-called 'external communications' under section 8(4) RIPA. It is now clear that section 8(4) warrants have been used as the basis for the mass interception by GCHQ of millions of private communications as well as its bulk collection of communications data.

There is no requirement for a warrant made under section 8(4) to be restricted in any way, unlike warrants under section 8(1) RIPA which must be targeted at either a particular person or a specific premises. Indeed, the government has since admitted that a section 8(4) warrant could include the interception of all communications between the United Kingdom and another city or country,[lv] for example all the emails, texts, phone calls, and internet communications between the UK and the United States.

The sole limiting factor for section 8(4) warrants is that they are directed at 'external communications', i.e. communications which either begin or end outside the UK.[lvi] In addition, the intelligence services are prohibited by section 16(1) from examining intercepted communications by reference to a person known to be in the UK.
However, it is now clear that the restrictions in section 8(4) offer no meaningful safeguard against the indiscriminate bulk interception of communications by GCHQ. For the very first time since RIPA was enacted, the government admitted in May 2014 that it understood the definition of 'external communications' to include any communications involving social media so long as the relevant server was outside the UK.[lvii]

"Internal" and "external" communications

We believe that the current distinction between 'internal' and 'external' communications under RIPA is both arbitrary and - in light of current technology - wholly antiquated. In an age when

communications between people in the UK routinely take place on US social media platforms any meaningful distinction between 'internal' and 'external' communications is not only discriminatory but nonsensical. The UK must afford all individuals – no matter their nationality or location, regardless of who they communicate with or how – the basic protections required by the rule of law.

Nor can the mass surveillance of private communications and the bulk collection of communications data without the requirement of reasonable suspicion be justified. If the requirements of targeting a specific person or premises are thought to be necessary safeguards for the purposes of a warrant under section 8(1), there is no justification for abandoning those safeguards in respect of so-called 'external' communications. Indeed, it is impossible to see how such indiscriminate surveillance could ever meet the requirement of proportionality, which is a fundamental part of the protection of the right to privacy.

In addition, the government has admitted that large numbers of 'internal' communications can also be swept up when intercepting so-called 'external' communications, because of alleged technical difficulties in intercepting communication network connections.[lviii] This is because the nature of internet-based communications means that it is generally impossible to determine - *at the point of interception* - whether a particular message is 'internal' or 'external' because many internal messages may be routed via other countries. In other words, millions of private messages between individuals in the UK are routinely intercepted by GCHQ under section 8(4) warrants because it is impossible to tell whether the messages are internal or external.

Section 5(6)

Whilst the government says excessive collection is due to the technical difficulty of separating data out, Section 5(6)(a) RIPA also allows government agencies too much latitude. It apparently includes capturing internal communications and communications data, which appears to be a major loophole:

"The conduct authorised by an interception warrant shall be taken to include (a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;
(b) conduct for obtaining related communications data; …"

Section 16

These problems with the arbitrary definition of 'external communications' under RIPA are

compounded by the lack of effective safeguards for bulk collection under section 8(4). The government has claimed that section 16 prevents the intelligence services from using section 8(4) warrants against UK citizens and residents. However, this is misleading. Section 16(2) only prevents GCHQ from searching the communications they intercept under section 8(4) where the communications are 'referable to a person known to be for the time being in the British Islands'. It does not prevent GCHQ from searching the same communications by reference to other factors, which may easily include people currently in the UK.

More importantly, section 16 places no restrictions whatsoever on the collection of communications data by GCHQ, regardless of whether or not the communication was internal or external and regardless of whether the person in question is known to be in the UK or not. Section 16 only restricts the use of the *contents* of messages intercepted by GCHQ. It places no restrictions on communications data. By relying on the broad scope of section 8(4) warrants to intercept millions upon millions of private communications, section 16 has enabled GCHQ to build up a vast database of the communications data of millions of UK residents which it can search at will without any clear legal authority or effective oversight.

Data Retention and Investigatory Powers Act (DRIPA)

As discussed above, the Government's rushed through this 'emergency' legislation in July 2014 with only three days of debate in Parliament. In particular, DRIPA does not address blanket data retention and the lack of independent authorisation of access, which were two of the key criteria identified by the CJEU in *Digital Rights Ireland* (see above). DRIPA should also be repealed and replace with legislation that complies with fundamental human rights.

In particular, in light of the CJEU ruling, it may be deduced that in order to comply with human rights law and EU law legislation must:

1) restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (see paragraph 59);
2) provide exceptions for persons whose communications are subject to an obligation of professional secrecy (see paragraph 58 of the judgment);
3) distinguish between the usefulness of different kinds of data and tailor retention periods on the basis of the data's possible usefulness for the purposes of the objective pursued or according to the persons concerned (paragraph 63);
4) ensure retention periods are limited to that which are 'strictly necessary' (paragraph 64);
5) empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);

6) restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);
7) limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);
8) ensure the data is kept securely with sufficient safeguards to ensure effective protection against the risk of abuse and unlawful access (paragraph 66);
9) ensure destruction of the data when it is no longer required (paragraph 67); and
10) ensure the data is kept within the EU (paragraph 68).

In our view DRIPA does not address the above numbered criteria: 1; 2; 5; 6; 7; and 10. DRIPA attempts to address criteria 3 and 4 by replacing a 12 month mandatory retention period with a 12 month "maximum" retention period. However, as retention notices served on service providers are not made public, it will be extremely difficult to assess whether in practice the notices are tailored and contain retention periods of lower than 12 months. We believe that new and comprehensive surveillance legislation is required and it must comply with the factors identified by the CJEU.

Six principles

We consider that the existing legislation should be replaced with legislation that reflects the six principles of the Don't Spy On Us coalition, of which ORG is a member. Currently surveillance law and practices fall short of these aspirations:

1) First, surveillance is only legitimate when it is targeted, authorised by a warrant, and is necessary and proportionate.
2) Second, whereas currently the Government uses secret agreements and interpretations of archaic laws, we need a clear legal framework governing surveillance to protect our rights.
3) Third, Ministers should not have the power to authorise surveillance. All surveillance should be sanctioned by an independent judge on a case-by-case basis.
4) Fourth, there should be effective democratic oversight. Parliament has failed to hold the intelligence agencies to account. Parliamentary oversight must be independent of the executive, properly resourced, and able to command public confidence through regular reporting and public sessions.
5) Fifth, innocent people have had their rights violated. Everyone should have the right to challenge surveillance in an open court.
6) Last, weakening the general security and privacy of communications systems erodes protections for everyone, and undermines trust in digital services. Secret operations by

government agencies should be targeted, and not attack widely used technologies, protocols and standards.

Legal challenge to RIPA and surveillance activity

Open Rights Group, alongside English PEN, Big Brother Watch and Constanze Kurz, instructed a legal team to pursue legal action on our behalf and on behalf of all internet users in the UK and EU. This resulted in a case being lodged at the European Court of Human Rights.

The case covers both GCHQ's TEMPORA programme and the receipt of data from the NSA's PRISM programme. The basis of our case is that UK surveillance practices are not sufficiently bound by UK law. The Court will decide whether the government's surveillance activities and the existing legislation sufficiently protect the privacy of UK and EU internet users.

We argue that the receipt by GCHQ of foreign intelligence data - such as information gathered by the NSA under the PRISM programme – does not appear to be covered by any laws or regulations in the UK. With regard to the TEMPORA programme, we argue amongst other things that the safeguards in RIPA sections 15 and 16 are insufficient and that the generic interception of external communications based simply on the transmission of information by transatlantic fibre- optic cables is inherently disproportionate.

We argue these activities fail the "in accordance with the law" and proportionality requirements of Article 8 ECHR.

On 16 January 2014, the Court wrote to the Government asking them to respond by 2 May to a number of questions raised by the case. The court also gave the case a rare priority designation. Further information and documents related to this legal challenge, including submissions made so far, supporting expert statements and the response from the court, are available from our website.[lix] The case is currently on hold pending the decision of the IPT in the Liberty and Privacy International case.

5. The statistical and transparency requirements that should apply

Increased transparency on the scale and reach of surveillance is necessary. Citizens must be sufficiently informed about the scope and nature of surveillance operations to be able to hold government to account. The government must begin to publish aggregate information on the number of surveillance authorisation requests approved and rejected so that citizens can understand the scale of surveillance requests made by the intelligence agencies and by

government agencies. Among other criteria, this data should contain a disaggregation of the requests by the service provider, including the investigation type and purpose.

Individuals should also be notified that they have been subject to surveillance after the event, unless there is a specific reason for maintaining secrecy, so that they may have the opportunity to bring proceedings to obtain an effective remedy for any violation of their right to privacy.

The US President's Review Group on Intelligence and Communications Technologies[lx] argued for increased transparency, with information about surveillance programs made available to the public 'to the greatest extent possible' and legislation that permits telecommunications companies to disclose information about the orders they receive from the government. They recommend 'civilian' involvement in the oversight of surveillance, alongside greater involvement for public interest advocates. And they conclude that the Government should be 'fully supporting and not undermining efforts to create encryption standards...'. We would also point to the draft report on the "US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", from the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, which includes a number of helpful recommendations.[lxi]

6. The effectiveness of current statutory oversight arrangements.

a) Intelligence and Security Committee

There must be concrete reform of the Intelligence and Security Committee (ISC) if it is to provide meaningful parliamentary oversight

The ISC has consistently failed in its duty to challenge the intelligence agencies. The Home Affairs Committee has concluded: 'we do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability, and to the credibility of Parliament itself'.[lxii] The operation of the ISC is hindered by non-disclosure. As Parliament's Joint Committee on Human Rights (JCHR) has noted, the level of redaction of ISC reports is sometimes so great that 'it can be difficult to follow the Committee's work and to understand its reports.'

To strengthen the ISC, the committee should have the status of a committee of Parliament, answerable directly to Parliament rather than to the prime minister. The ISC must take its own decisions on reporting and publication. The committee must be appropriately funded and staffed with independent experts able to undertake detailed forensic investigations and an independent

secretariat, including independent legal and technical advice. The committee should have strengthened legal powers to require the production of information and to compel the attendance of witnesses. In accordance with recommendations by the Home Affairs Committee, the chair of the committee should be a member of the largest opposition party and the Commons members of the committee should be elected.[lxiii]

b) The commissioners

The offices of the Intelligence Services Commissioner and the Interception of Communications Commissioner should be reformed. Both should report to Parliament and be insulated from executive influence.

In the absence of prior judicial authorisation for surveillance decisions, it is vital that all decisions be subject to ex post facto scrutiny by a judge. Unfortunately, however, the Interception of Communications Commissioner inspects only a small proportion of warrants made by the Secretary of State, somewhere between 5 per cent to 10 per cent. The Commissioners have not publicly found a warrant to be disproportionate and are under-resourced. The roles should be full time and better-resourced. The Intelligence Services Commissioner has also consistently refused to publish statistics on warrants or authorisations issued to the Security and Intelligence Services.

If the Commissioners are to offer effective oversight, they must be empowered to conduct searching investigations, with adequate resources and the requirement to publish key statistics.

October 2014

i. http://ico.org/for_organisation/privacy_and_electronic_communications
ii. http://www.zeit.de/datenschutz/malte-spitz-data-retention
iii. http://www.pnas.org/content/110/15/5802.full.pdf+html
iv. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
v. http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation
vi. http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents
vii. http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden
viii. http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
ix. http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?commentID=washingtonpost.com/ECHO/item/1386720327-479-532#whitepaper
x. http://www.washingtonpost.com/world/national-security/nsa-tracking-phone-locations-on-planetary-scale/2013/12/05/dfe21740-5db2-11e3-bc56-c6ca94801fac_story.html
xi. Loch K. Johnson, Richard J. Aldrich, Christopher Moran, David M. Barrett, Glenn Hastedt, Robert Jervis, Wolfgang Krieger, Rose McDermott, Sir David Omand, Mark Phythian & Wesley K. Wark (2014): An INS Special Forum: Implications of the Snowden Leaks, Intelligence and National Security, DOI: 10.1080/02684527.2014.946242
xii. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf
xiii. https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/open_govt_response.pdf
xiv. http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world
xv. https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness_st_of_charles_blandford_farr.pdf
xvi. http://www.statewatch.org/news/2014/apr/interception-comms-code-practice.pdf
xvii. http://www.bbc.co.uk/news/uk-politics-24848186
xviii. http://www.legislation.gov.uk/ukpga/2000/23/section/16
xix. https://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf
xx. http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
xxi. https://www.nsa.gov/research/_files/tech_transfers/nsa_technology_transfer_program.pdf
xxii. https://www.nsa.gov/research/tnw/tnw193/article2.shtml
xxiii. https://www.facebook.com/publications/225061261024135/
xxiv. http://googleblog.blogspot.co.uk/2012/06/using-large-scale-brain-simulations-for.html
xxv. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

xxvi. http://www.bbc.co.uk/news/uk-politics-24848186

xxvii. Amoore, L. (2013). *The Politics of Possibility*. *Risk and Security Beyond Probability*. Duke University Press.

xxviii. http://www.mynewsdesk.com/uk/pressreleases/home-office-government-ramps-up-passenger-screening-382694

xxix. Interview with Louise Amoore, in above.

xxx. Amoore, L., & de Goede, M. (2008). *Risk and the War on Terror*. Taylor & Francis.

xxxi. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

xxxii. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311126/PartnerBulletinFebruary.pdf

xxxiii. http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document

xxxiv. see e.g. *Copland v United Kingdom* App no. 62617/00, 3 April 2007

xxxv. *S and Marper v the United Kingdom*, Applications nos. 30562/04 and 30566/04

xxxvi. *Kennedy v UK* (2011) 52 EHRR 4 at [93]

xxxvii. Liberty v UK (2009) 48 EHRR 1

xxxviii. Section 3(2) Interception of Communications Act 1985

xxxix. *Riley v California*, 573 US (2014) at 19.

xl. David Cole, 'We Kill People Based on Metadata', New York Review of Books (10 May 2014).

xli. Ibid.

xlii. Judgment in Digital Rights Ireland case (joined cases C-293/12 and C-594/12) available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, paragraph 65

xliii. Paragraph 59

xliv. Paragraph 62

xlv. Paragraph 59

xlvi. Paragraph 58

xlvii. Paragraphs 63 – 64

xlviii. The Data Retention Regulations 2014

xlix. Paragraphs 60 -62 of *Digital Rights Ireland* judgment

l. Paragraphs 66 - 68

li. The Investigatory Powers Tribunal website, 'Operation – Cases Upheld', http://www.ipt-uk.com/section.aspx?pageid=9

lii. How the NSA's MUSCULAR program collects too much data from Yahoo and Google', Washington Post (October 2013), http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/

liii. Nick Hopkins and Julian Borger, 'Exclusive: NSA pays £100m in secret funding for GCHQ', The Guardian (1 August 2013), http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

liv. Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al, IPT/13/92/CH, The Respondents' Open Response,

https://www.privacyinternational.org/sites/privacyinternational.org/files/litigations/open_govt_response.pdf

lv. See para 194.3 of the Government's Open Response to the claims brought by Liberty and Privacy International before the Investigatory Powers Tribunal in relation to Prism and Tempora.

lvi. See section 20 RIPA.

lvii. See the statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, dated 16 May 2014, at para 137.

lviii. Statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, 16 May 2014, at para 44

lix. https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-internet-surveillance/

lx. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

lxi. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN (see page 19)

lxii. Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 157, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

lxiii. Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 158, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

Charles Raab

Intelligence and Security Committee of Parliament
Privacy and Security Inquiry

This submission is from Professor Charles D. Raab, Professor of Government in the School of Social and Political Science, University of Edinburgh. My academic teaching and research has concerned privacy, processes involving personal information, surveillance, and the regulatory and governance arrangements that relate to these. I am not a specialist in the security and intelligence services, although some of my work on the above topics is relevant to their activities. I am writing in my personal capacity.

Executive Summary

This submission is limited largely to addressing guidelines 6(a) and 6(b) of the Call for Evidence. It draws attention to ambiguities in the terms used: 'privacy', 'security', 'collective security', 'individual right', and 'balance'. It argues that clarity in the use of these terms is important in opening up new and more complex insights into what is at stake in the relationship between the security and intelligence services and the public, and in the performance of effective scrutiny and oversight. It considers that a better grounding is needed so that more nuanced criteria for judgment can be applied to these security and oversight tasks. It refers to some current proposals from the USA that might inspire comparable measures to place oversight on a better and more transparent basis, potentially leading to greater public confidence.

Submission

1. I welcome the Intelligence and Security Committee's (ISC) attempt to broaden its inquiry into the legal framework for the interception of private communications. I would urge it to use its special knowledge of the formal internal organisation, procedures, and norms of intelligence agencies to widen its canvas in order to include inquiry into these extra-legal matters insofar as they might lead to the improvement of its scrutiny of the work of these agencies.

2. It is vitally important that the laws, administrative arrangements and normative cultures in this exceptionally difficult and sensitive field enjoy public confidence and. In a democracy , the public's support for legitimate state security and intelligence work is crucial, so that they see this work as being can-ied out in their interest and not as the operations of security services who regard citizens as suspicious potential agents of terror, crime and other threats to the state and society. However, these relationships between the citizen and the state may have been damaged especially by recent surveillance revelations and allegations emanating from the Snowden episode.[1] A significant proportion of public and informed opinion now registers doubts that the security services are sufficiently under control and are

[1] In the pre-Snowden era, the implications of surveillance, albeit not of national security, for citizens were investigated in *Surveillance: Citizens and the State,* House of Lords, Select Committee on the Constitution, 2"d Report of Session 2008-09, HL Paper 18.

operating within justifiable limits consonant with robust estimates of threats to national security and public safety.

3. These are questions of public perception that may not necessarily reflect the reality of how these services act and think, but perceptions are important and the services, as well as their overseers, must aim to dispel any unwarranted conceptions through as much transparency as possible. Public control and oversight through elected representatives and accountable appointees is an essential principle in a democracy, and can be a vehicle for transparency. The processes of independent scrutiny can play an essential part in reinforcing justifiable public support through investigation, questioning, and scepticism. Mediating between the public and the intelligence and security services, the ISC could play a vital part in helping to restore, or to establish, a high level of public confidence. It could do this through an enhanced role in making intelligence and security activities more transparent and accountable, consistent with the interests of effectiveness, and in exercising its judgment to criticise practices that have a negative effect on rights and liberties. In this judgment, the principles of necessity and proportionality should be applied rigorously and independently, and their application should be open, as far as possible, to interrogation and challenge at relevant stages of the security and intelligence activities concerned. This may be a matter for legislation, but also for the internal governance of agencies and for external scrutiny machinery. Transparency should be a main criterion for the improvement of present arrangements.

4. The Call for Evidence asks: 'What balance should be struck between the individual right to privacy and the collective right to security?' I believe this formulation of the issue is mistaken, rhetorical and imprecise; it impedes a deeper understanding of what is at stake for the individual, society and the state. Principles underlying the work of scrutiny, and judgments of the legitimacy of surveillance and security operations, would be better grounded if alternative ways of construing the relationship between security and privacy were understood and incorporated into practice. The following paragraphs examine this.

5. Three difficulties can be identified here. The first one is the way in which 'privacy' is construed. Privacy is indeed an individual right: fundamental but not absolute, and enshrined in prominent national and international legal instruments. However, privacy's importance goes beyond that of the individual, as is argued at the leading edge of academic and legal commentary. Privacy is acknowledged to be a crucial underpinning of interpersonal relationships, of society itself. and of the workings of democratic political systems.[2] To consider privacy only as an individual

[2] Among many other sources, see Solove, D. (2008) *Understanding Privacy,* Cambridge, MA: Harvard University Press; Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy,* Chapel Hill, NC: University of North Carolina Press, eh. 8; Nissenbaum, H. (20 I 0) *Privacy in Context: Technology, Policy. and the Integrity of Social Life,* Stanford, CA: Stanford University Press; Goold, B. (2009) 'Surveillance and the Political Value of Privacy', *Amsterdam Law Forum* I (4), http://amsterdamlawforum.org; Cohen, J. (20 12), *Configuring the Networked Self: Law, Code, and the Play of Everyday Life,* New Haven, CT: Yale University Press; Schoeman, F. (1992) *Privacy and Social Freedom,* Cambridge: Cambridge University Press; Steeves, V. (2009) 'Reclaiming the Social Value of Privacy', in Kerr, I., Steeves, V. and Lucock, C. (eds.), *Lessons From the Identity Trail: Privacy, Anonymity and Identity in a Networked Society,* New York, NY: Oxford University Press; Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective,* Cambridge, MA: MIT Press, eh. 2; Raab, C., (2012) 'Privacy, Social Values and the Public Interest', in Busch, A. and Hofmann, J. (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Baden-Baden : Nomos

right is to ignore its value in these other dimensions, and thus to lose sight of its fuller significance in theory and practice. When individual privacy is protected, the fabric of society and the functioning of political processes and the exercise of important freedoms are thereby protected. When it is eroded, society and the polity are also harmed; it is in the public interest, and not only in the interest of the individual, to protect privacy. The individual right may be infringed for legal and legitimate reasons, such as the overriding importance of other rights and interests, but the claims of the latter to supervene must be argued and not merely asserted, must not be permanently accepted, and may ultimately be a matter for judicial determination. The unfortunate example of societies and of individuals under totalitarian or authoritarian governments serves as a reminder of the importance of these points.

6. The second difficulty lies in the common and repeated assumption made by politicians, the media, and the general public, that the issue is one of 'national security' *versus* 'personal privacy'. In practice, this assumption typically leads to the conclusion that this 'collective right' must normally trump the 'individual right' to which it is thought to be opposed. It is very difficult to counter this, especially in the present climate of fear. *This* is unfortunate, especially when the collective value of that individual right can also be seriously considered to be important, as explained above. The precedence taken by national security offers little scope for solutions that are more consistent with articulating the kind of society and polity we wish to sustain. Construing security and privacy as opposed also fails to recognise that both collective security and individual privacy are two expressions of a public interest, as argued above, and of the nature of the rights in question; this failure points up the facile nature of the supposed antagonism as a general principle.

7. A similar argument has been made about the relationship between security and liberty. A strong case can be supported for scepticism about whether seeing these values or rights as at odds is a proper way of looking at it.[3] In an atmosphere of fear of terrorist and other attacks, the conflictual way in which the relationship between security and liberty (or privacy) is presented has rhetorical force and supports arguments in favour of security practices and organisations far more than it does for liberty or privacy protection and the regulation of infringement. The interests that seek to perpetuate this predominance are stronger and louder than those who would challenge it and seek other kinds of reconciliation.

8. This is where independent organisations for regulation and scrutiny can play a crucial role in creating a level playing-field for the interests involved and in ensuring that there should be no presumption in favour of one side of the argument. But they can also play a crucial role in scepticism about whether the 'argument', if any, is correctly stated: that is, the claim that national security and privacy are antagonists, and that the former must prevail because of the way the 'collective' is construed. Where the old quips, 'better safe than sorry', 'there are no votes in privacy' and 'privacy is dead', are still recited in governmental and commercial sectors, it is important to have some means of offsetting the facile assumptions that often underlie policy and practice in the security field. Nor is it persuasive, on grounds of principle and rights, to claim glibly that 'the public doesn't care about privacy', as if the

---

Verlagsgesellschaft.

[3] See the critical and sceptical arguments in Waldron, J. (2003) 'Security and Liberty: The Image of Balance', *The Journal of Political Philosophy,* vol. 11, 191-210; Loader, I. and Walker, N. (2007) *Civilizing Security,* Cambridge University Press, 54-56.

exercise and validity of rights should depend on the state of public – even majority – opinion as ascertained in surveys, themselves difficult to interpret and often severely flawed. [4]

9. In this regard, it may be useful to draw inspiration from the recent report published by President Obama's Review Group on Intelligence and Communication Technologies,[5] a group established to determine how the protection of national security and respect for privacy and civil liberties can both be accomplished in the circumstances of intelligence operations following the Snowden revelations. Whilst the United States and the United Kingdom are considerably different in their governmental machinery and policy processes so that it would be difficult for the UK to transpose major structural innovations directly, the spirit and intent of the Review Group's recommendations command attention.

10. Two of its recommendations in particular are worth noting. Recommendation 26 calls for 'the creation of a privacy and civil liberties policy official located both in the National Security Staff and the Office of Management and Budget'. Separate from compliance, such an official would co-ordinate privacy policy within government, 'including issues within the intelligence community ... [and] ensure that privacy issues are considered by policymakers.' The official would provide 'a focal point for outside experts, advocacy groups, industry, foreign governments, and others to inform the policy process.'[6] Whatever the machinery might be for giving effect to this idea in our country, having such a role performed at the centre of security policy-making, management and oversight would provide a counterweight to those interests that might undervalue the importance of privacy and civil liberties in their programmes and operations.

11. Recommendation 27 calls for a Civil Liberties and Privacy Protection Board to 'oversee Intelligence Community activities for foreign intelligence purposes, ratherthan only for counterterrorism purposes'. It would also 'be an authorized recipient for whistle-blower complaints related to privacy and civil liberties concerns from employees in the Intelligence Community '. Moreover, the creation of an Office of Technology Assessment within the Board is considered useful 'to assess Intelligence Community technology initiatives and support privacy-enhancing technologies'.[7] As the Report states, '[a]n improved technology assessment function is essential to informing policymakers about the range of options, both for collection and use of personal information , and also about the cost and effectiveness of privacy-enhancingtechnologies.'[8]

12. Inspired by these recommendations, innovations tailored to the circumstances of our government could provide important means for augmenting the UK's slender oversight and scrutiny machinery. They would create additional capacity and

---

[4] Public opinion surveys of attitudes towards privacy and security have been examined in the PRISMS project conducted under the European Union 7th Framework Programme, in which the author participates.

[5] *Liberty in a Changing World,* Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,12 December 2013.

[6] Ibid., pp. 194-5.

[7] Ibid., p. 195. Privacy impact assessment (PIA) has become a widespread technique for information systems and technologies; see Wright, D. and De Hert, P. (eds.) (2012, *Privacy Impact Assessment,* Dordrecht: Springer. Among the organisations that conduct PIA is the USA 's Department of Homeland Security :see https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia.

[8] Ibid ., p. 198.

functions with which government would not only be able to implement its concern for privacy and civil liberties in the midst of security processes, but also to be seen to be doing this in an open and accountable way. To be sure, this might entail constitutional changes in our system that have implications wider than those for the intelligence and security services alone. But, in part, they relate to guideline 6(b) of the ISC's Call for Evidence in dealing with the apparent need to review the legal framework in response to developments in information technology. They also resonate with guideline 6(a) by suggesting a way in which the claims of privacy protection could be more effectively represented in the highest counsels of government, and in which a wider policy relevant discourse on privacy might be facilitated.

13. The third difficulty lies in the way 'security' is construed. As with privacy, there are many ways of understanding this – or its cognate, 'public safety' – and whatever right is considered to pertain to it, as well as its relationship to other rights.[9] Leaving aside the question of individual or personal security, one issue is that 'collective' security could refer to security at a variety of levels: for example, international, national, local, neighbourhood, or social group. How the claims of each of these might be promoted in the light of the right to privacy (itself of diverse meanings), and thus the nature of any reconciliation, will vary. Another issue is whether objective security – involving probabilities of risk – and/or subjective security – involving feelings of insecurity – should be at the focus of attention, and how these two foci can be reconciled.[10] A further issue is whether privacy and civil liberties (or freedoms) should not themselves be regarded, at least in some respects, as valuable because of the security and safety – not least, of personal data – they provide for individuals, groups and societies. If so, their relationship to each other is far more complex and cannot be glossed over by a rhetoric of the 'opposed' rights or values of security and privacy.[11] This observation is reflected in President Obama's Review Group's remark that '[t]he United States Government must protect, at once, two different forms of security: national security and personal privacy'.[12]

14. It follows that, if both privacy and security are contested and inter-related concepts, the idea that they can be 'balanced' or 'traded-off' must also come under sceptical scrutiny.[13] President Obama's Review Group noted that '[t]he idea of "balancing" has an important element of truth, but it is also inadequate and misleading'.[14] Whether 'balancing' is between one individual right and another, or

---

[9] See Zedner, L. (2009) *Security,* London: Routledge; Zedner, L. (2003) 'The Concept of Security: An Agenda for Comparative Analysis' , *Legal Studies,* vol. 23, 153-175; Zedner, L. 'Seeking Security by Eroding Rights: The Side-stepping of Due Process ', Fredman, S. 'The Positive Right to Security', and Lazarus, L. 'Mapping the Right to Security', all in Goold, B. and Lazarus, L.(eds.) (2007) *Security and Human Rights,* Oxford: Hart Publishing.

[10] Chandler, V. 'Privacy Versus National Security: Clarifying the Trade-off , in Kerr *et al.* (eds), op. cit.

[11] Raab, C. (2014), 'Privacy as a Security Value', in Bekken, A., Schartum, D. and Bygrave, L. (eds.) *Jon Bing: A Tribute,* Oslo: Gyldendal.

[12] *Liberty in a Changing World,* op. cit., 14.

[13] See van Lieshout, M., Friedewald , M., Wright, D. and Gutwirth. S., (2013) 'Reconciling privacy and security', *Innovation – The European Journal of Social Science Research* vol. 26, nos. 1-2, 119-132. This is the focus of attention of the PRISMS project conducted under the European Union 7th Framework Programme, in which the author participates.

[14] *Liberty in a Changing World,* op. cit, 16. The Panel nevertheless continues to use the term in developing its Recommendation s. See also Dworkin, R. (1977) *Taking Rights Seriously,* London : Duckworth; Waldron, op. cit; Raab, C. (1999) 'From Balancing to Steering: New Directions for Data Protection', in Bennett, C. and Grant, R. (eds.), *Visions of Privacy: Policy Approaches for the Digital Age,* Toronto: University of Toronto Press.

between an individual right and a collective right, or between an individual right and social or collective utility, also requires specification and precision if 'balancing· – even if inescapably built into our mindset – is to be taken away from the realm of shorthand and slogan.

15. In any case, the assumptions about equilibrium and about a supposed common metric for weighing are not clear and are doubtfully warranted. Is it suggested that we can know, and can all agree, how much (and whose) privacy should or should not outweigh how much (and whose) security? In addition, the proposal to engage in balancing is by itself silent about the method by which a balance can be determined and challenged, and about who is to determine it. Moreover, whether 'balance' refers to the method, or to its outcome, is often left unexplained by its proponent s. The published decisions in legal cases are one source for understanding, and perhaps disputing, the weighing process and the arguments used, for instance about necessity and proportionality. It remains to be seen how these understanding s can be disseminated in the much more closed conditions of the intelligence and security service where strategic and operational decisions have to be made, and also brought tobear in their oversight and scrutiny.

16. In conclusion, perhaps a better question for the Committee to ask would be: 'in combating terror and other threats, how can we ensure that, by applying more nuanced understanding, the claims for security measures are not the default when other values and rights are also at stake?' In carrying out their scrutiny, those who exercise regulatory and oversight functions must ascertain the purpose and effectiveness of security and intelligence service activities as well as their necessity, proportionality , legitimacy and legality. They must also press those services to show how they have justified their operations by means of these criteria, and have taken seriously the likely effect upon privacy and liberty construed as broadly as possible. They should also, and perhaps in the first instance, clarify and find means to widen the debate about the meaning of 'privacy', and especially of 'security' and 'national security'; and about how surveillance and intelligence activities affect the achievement of these objectives. This would help to move these terms, as well as security policy and practice, away from the realm of automatic acquiescence in invasive surveillance and towards constructive and critical public and parliamentary debate about the rights that are involved, yet consistently with the justifiable secrecy that surrounds strategy and operations. How transparency and secrecy can themselves be reconciled is in itself, of course, a matter for debate. But public confidence may be the ultimate beneficiary of all these processes of thinking and decision; in the long run, this confidence may be the most essential touchstone for security policy.

February 2014

Rights Watch (UK)

1. **Our Mission:** Promoting human rights and holding governments to account, drawing upon the lessons learned from the conflict in Northern Ireland.

2. **Our Expertise and Achievements:** Since 1990, Rights Watch (UK) (formerly British Irish Rights Watch) has held the UK Government and non-state actors to account for human rights abuses in conflict settings. We work with victims and communities to expose human rights abuses, to obtain redress and to hold those responsible for such abuses to account. Our interventions have reflected our range of expertise, from the right to a fair trial to the scope of the government's investigative obligation under Article 2 of the European Convention in Human Rights. We have a long record of working closely with Non-Governmental Organisations (NGOs) and government authorities to share that expertise. And we have received wide recognition, as the first winner of the Parliamentary Assembly of the Council of Europe's Human Rights Prize in 2009 alongside other honours.

3. We have experience of working with communities and individuals who believe that they have been subject to undue surveillance. We have commented on the interception of communications data including in written submissions to the Privacy and Security Inquiry of the Intelligence and Security Committee of the House of Parliament, we will giving additional oral submissions to this inquiry on 15th October.

4. We will make submissions on the following issues regarding the use of communications data and interception found in the terms of reference of the Review of Communications Data and Interception Powers :
   - The safeguards to protect privacy;
   - The case for amending or replacing the legislation;
   - The statistical and transparency requirements that should apply; and
   - The effectiveness of current statutory oversight arrangements.

5. **Issues with the current regime**
   Many individuals and communities feel that they have been subject to unwarranted surveillance of their activities due to perceived links to terrorist groups. These groups have consistently expressed concerns to us that the regime for monitoring

the interception of communications data is inadequate as it lacks sufficient safeguards. Currently the safeguards regime is fundamentally flawed as:

- There is little independent oversight of the interception of communications data
- What oversight there is not transparent; and
- There is a lack of clarity as to what actions are permitted under the law

6. The interception of communications data is carried out under the Regulation of Investigatory Powers Act 2000. This regime provides for a system of internal oversight of the decision to make authorisations and notices to obtain communications data, overseen by the Interception of Communications Commissioner. The Commissioner has a small team of 9 inspectors; they had to contend with 514,608 notices and authorisations in 2013 alone. Such a ratio makes it impossible for the Commissioner to assess a significant proportion of the notices and authorisations made undermining the oversight he can provide. This means in the majority of cases that there will be no outside scrutiny of a decision to intercept communications data. This makes it difficult for members of the public to have confidence in the system of oversight and regulation.

7. This issue is compounded by the fact that individuals' who wish to challenge the possible interception of their communications data can only do so through the Investigatory Powers Tribunal (IPT). This can be a difficult and frustrating procedure due to the lack of transparency in the way the tribunal operates. Lawyers and communities have therefor lost confidence in the Tribunal, meaning that they are unwilling to bring cases to the Tribunal as they do not believe that they will get a fair hearing. Individuals' have reported concerns that bringing a case would lead to increased surveillance rather than providing them with protection from this. Whilst it is understandable that the IPT must operate in such a way as to not undermine the activities of the police and security services, it must also ensure that justice is seen to be done if it wishes to deal with the lack of confidence in its impartiality.

8. The Interception of Communications Commissioner states in his 2013 report:

> *'I have very considerable sympathy with those who are hazy about the details of the legislation. The Regulation of Investigatory Powers Act 2000 (RIPA 2000) is a difficult statute to understand…..Because RIPA 2000 Part I is difficult legislation, this narrative may in places be dense and perhaps itself indigestible. I have tried to make it as accessible as possible, but apologise if I have not entirely achieved this.'* Section 1.6

The lack of clarity in the law makes it difficult for those commissioning the interception of communications data to ensure they are doing so within the law and

for those scrutinising the interception to ensure that it has occurred properly. If those who work with these powers on a regular basis find them difficult to use or explain, then it is understandable that the general public are likely to feel that there are no effective safeguards in place to ensure that their communications data is not intercepted illegitimately.

9. Overall therefore the system is currently inadequate as it fails to ensure that there are safeguards in place that give confidence to the public that interception of communications data powers are not misused. This is particularly important among communities who are considered suspect due to the involvement of some of their members with terrorist activity. Our experience from Northern Ireland indicates that when communities lose faith in the oversight and monitoring agencies this causes them to disengage from efforts to co-operate with policing. Instead communities feel victimised which adds to their sense of alienation. This provides fertile ground for extremist and radical ideologies to take root, undermining the security of the United Kingdom, the very situation that conferring such powers seeks to prevent.

10. **Proposed amendments that would make the law more effective**

    To restore public confidence, especially amongst suspect communities, what is needed is a more open and accountable system, where justice is seen to be done. We would therefore suggest the following changes:

    - Independent oversight of all authorisations and notices relating to communications data
    - A simplified statutory regime to make it clear in what circumstances communications data can be accessed by governmental bodies
    - Taking additional steps to ensure that that the IPT appears to be (and is) independent.
    - Providing more detailed statistics that clarify how communications data is used in general by accessing bodies.

11. The Interception of Communications Commissioner's office should be better funded so as to enable them to increase the level of staffing to ensure that all requests to access communications data are scrutinised by an independent body. This would add a level of oversight that would ensure that cases of misuse are minimised, and promote best practice. It would also give the public greater confidence that the powers to intercept communications data were not being misused.

12. A single set of rules governing the interception of all communications data, regardless of its origin, route of communication, and end point would improve the transparency of the regime. It would ensure that the regime is clear for those who

use it, scrutinise it and are subject to it. This would promote greater confidence in the system as it would be more easily understood by ordinary individuals.

13. The Investigatory Powers Tribunal requires significant reform for it to be considered a trustworthy court by many. Firstly, its rules procedure and membership should not be subject to the discretion of the Secretary of State as this significantly contributes to the perception that is the IPT is not independent from the Government. Secondly, individuals should be able to appeal their cases from the IPT to a higher court, accepting that this appeal may have to be heard using closed material procedures. The lack of right to appeal also adds to a perception that the tribunal is not an independent body, but simply a dead end with which to confound legitimate complainants. Thirdly, the IPT should provide more clarity as to how it operates and how it comes to its decisions. This will provide more transparency and accountability for the tribunal and help restore public confidence.

14. Currently the statistics relating to the interception of communications data are at a high level, providing only a breakdown by overarching justification of the authorisation; what type of public body made the authorisation or notices and as to what type of data was intercepted. The Interception of Communications Commissioner concedes that these statistics are inaccurate due to the way that different public bodies record each authorisation. This should be rectified by clear reporting standards for all public bodies ensuring uniformity of reporting and clarity of statistics. The statistics should also go into greater depth, for example explaining how many authorisations are made to access the communications of individuals who are imprisoned, on bail or subject to Terrorism Prevention and Investigation Orders, compared to those used for investigations. Disclosure of these statistics would not endanger national security as they could not be used to inform individuals about specific cases, but would give more clarity to the public as to how public bodies use communications data.

October 2014

Roke Manor Research Ltd

Roke Manor Research Ltd ('Roke') is part of Chemring Group plc, a UK Defence & Security company supplying high technology electronics and energetic products to over 60 countries globally. Prior to Chemring's acquisition in 2010, Roke lead research and developed into network infrastructure and mobile handsets for Siemens Mobile Communications business for both the 2G and 3G standards. Roke is still actively at the leading edge of telecommunications research. For instance we are an active member of the 5G Innovation Centre based at Surrey University.

Today, Roke is a supplier of commercial products, bespoke hardware and software capabilities, and technical consultancy. Roke's customer base includes international telecommunication organisations, UK Government and selected foreign Governments. Roke has been a leading UK provider of Lawful Intercept capability and consultancy since RIPA Legislation received Royal Assent in 2000. Roke has also provided technology consultancy into the Home Office's CCD programme since its inception (when it was the Interception Modernisation Programme).

The Investigatory Powers Review ('Review') has requested written evidence of issues relating to the Terms of Reference below, and the independent insight we feel we can provide against each of the objectives is highlighted in **bold** and detailed in the remainder of this document.

1. **Current and future threats, capability requirements and the challenges of current and future technologies;**
2. **The safeguards to protect privacy;**
3. **The implications for the legal framework of the changing global nature of technology;**
4. The case for amending or replacing the legislation;
5. The statistical and transparency requirements that should apply; and
6. The effectiveness of current statutory oversight arrangements.

1. Current and future threats, capability requirements and the challenges of current and future technologies

This section details some of the current and future technologies and related issues that Roke believes should be considered within the Review process. Not all new technologies disrupt equally, so it is crucial to understand how they will disrupt within a Law Enforcement context.

Capabilities that could potentially be called upon to safeguard the interests of the nation and the individual, either now or in the future, can be described under the following four capability areas.

a. Lawful/legal Interception, and Signals Intelligence – The collection of wired and wireless signals;
b. Seized Media Forensics – The investigation and analysis is seized media such as memory sticks, hard-drives, mobile devices and other forms of data storage devices including server centres;
c. Open Source Intelligence – The collection and investigation of publically available material including books, posters, pamphlets, websites;
d. Computer Hacking – The manipulation of a specific electronic device for the purpose of collecting evidence or intelligence.

All current law enforcement capabilities can be described within this framework. Before the trends and threats driving each of these capability areas are discussed, it is interesting to note that these capabilities, while once separated, are now clearly beginning to converge. The legislation governing each area will be challenged by this convergence. Conversely, capabilities that once operated successfully in isolation will become irrelevant if a blended approach cannot be found. For example, police forces have a deliberately restricted pallet of capabilities, most importantly seized media forensics. However the value of this capability is rapidly in decline. Without support from other capability areas the police will cease to be effective with regards to eCrime.

a. Lawful/legal Interception, and Signals Intelligence

The value of LI/SigInt is falling year on year as the UK "sees" less and less of less and less. This is to say that the percentage of global communications flowing through the UK is continuously falling. Fibre with effectively infinite bandwidth is being laid around Africa, through the Mediterranean, and between India and China.

Secondly, this trend is concurrent with the rise in effective and resilient encryption. Previously, encryption was difficult to implement correctly (and often wasn't), and expensive to develop. Online encryption was slow and badly effected user experience. Today encryption is implemented professionally and can be supplied for little or no cost. For example, Facebook loading times for the encrypted service is only 300ms slower than the unencrypted page.
Already "traffic analysis" and the analysis of metadata have been turned to, but offer a far poorer alternative in real terms.

It is clear that significantly greater volumes of lower quality data will be required just to stand still in this space; even this undertaking is an extremely challenging task for technology. Increasing stored data volumes will be a natural consequence and response to these trends, further accelerated by the exponential increase in internet use.

A key point for consideration should be the difference between data volume and data value. It is predicted that any future technology in this area will require an information distillation process. Additionally, such a process will likely require much lower grade data from many more unrelated individual parties in order to provide a small amount of valuable information about a small number of relevant parties. This approach is likely to become necessary. The unrelated parties are protected by the same mechanism as the summation of their specific data offers little or no information value.

b. Seized Media Forensics

There are no technology drivers supporting the use of local storage of information. All technology drivers point to data being stored remotely in a distributed manner. Such distributed storage allows for redundancy, resilience, economies of scale, ease of access and the generation of new products and services. Marketers, advertisers and information service providers all aim for data aggregation and creation of data in a virtualised and distributed "always on" environment.

The seizure and investigation of a specific electronic device such as a smart phone or a home computer is offering less and less evidence and intelligence value. "Over the Top" apps intend to provide a user access to data or a service from any device anywhere in the world. This is achieved by storing all of the users data "off device" in a virtual cloud

environment. Webmail was one of the first examples of such a service. Additionally, many devices can be remotely wiped by the user, or support professional grade encryption by default.

Today's legislation allows police forces to demand a user's password to an encrypted file, however software freely available such as TrueCrypt allows users to have several valid passwords for a single encrypted file, with each password decrypting the file in a different manner. This allows an individual to relinquish a single password to meet their legal obligations, while at the same time not acknowledging the existence of other decryption keys. It is mathematically impossible to discover the existence of such "hidden volumes" offered by such software.

c. Open Source Intelligence

The public disclosure of information is now common place on the internet, or in other mediums. Commercial organisations collect and analyse such data in massive quantities. However law enforcement agencies cannot and are prohibited by law. Online disclosure of information is highly likely to continue to increase with more and more data being shared openly online. In this domain, information value is exceptionally high owing to the data being specific and relating to a named entity or individual.

The danger to individual's privacy is acute. The deep question to be asked in this area is how best to address the "aggregation problem". In the first instance, elements of data can be reviewed in isolation from the rest of the data corpus. Information commissioners can inspect the impact of collecting and storing a specific fact, or type of data. However, when the data is aggregated, no one currently understands the full extent of what can be additionally inferred, and what the real value for the data actually is. What is known is that the value of specific data when considered as a set is far greater than the risks posed by any specific fact. This is currently a major topic for research institutions, think-tanks and marketeers.

d. Computer Hacking

The most specific and most targeted capability would be the concept of gaining access, and/or control of an individual's personal device, or the devices of an entity/organisation. What is known is that progressively more complex systems will always have emergent properties and implementation flaws that will continuously facilitate such activities irrespective of antivirus measures.

Commercial organisations historically have favoured to roll-out a product or service quickly and secure it later, however, this comment must be tempered by new products and services suffering from new flaws that no organisation could have foreseen and/or prevented. As the value of LI/Sigint and seized media forensics diminishes, organisations will turn more and more to computer hacking for either a substitute capability, or as a mechanism to maintain and support the other declining areas. Orphaned capabilities operating in isolation will diminish as a blended approach becomes the only viable approach.

2. The safeguards to protect privacy

The risks to privacy posed by the capabilities listed above are not equivalent. In all cases there is an important difference between data volume and data value. It is clear that with regards to

LI/Signit data volumes are set to increase while the total value offered by the data actually falls in real terms.

Some capabilities suffer from fundamental scaling challenges such as seized media forensics. Seized media is also likely to see a continuation of the fall in total data value. The two capabilities that pose more concerning privacy challenges is computer hacking and open source intelligence collection.

The information aggregation challenge remains unaddressed and is likely to do so for the foreseeable future. The Knightian "unknown unknowns" will remain a continual privacy challenge as new and innovative data analysis developments are likely to outstrip public and government understanding for some time to come.

Reviews of data holdings are likely to become extremely miss-leading. In some cases vast quantities of data held on millions of individuals will yield little value, but will be vital to an information distillation process. In other cases such as open source intelligence, a small number of carefully interpreted facts will reveal intimate details of private life relating to health, lifestyle, sexual preference and financial position.

Questions should be asked about information systems "intent" and take a holistic view of the overall process. At the same time questions of system misuse should be carefully reviewed in terms of both misuse by an individual, as well as misuse by a controlling authority. Management and monitoring of processing and analysis systems will become far more critical than absolute database sizes and data types.

Additionally, it is a question as to how frequently a specific record is actually accessed. Data Retention periods require "right-sizing". Auditing data usage could be the key to understanding how best to gauge retention periods and the value of storing the data.

3. The implications for the legal framework of the changing global nature of technology

a. A Global Perspective

The internet facilitates near perfect information liquidity. Information flows near instantly around the globe. Current storage technologies aim at providing data resilience, this can and is being achieved by fragmenting files cross multiple storage devices, potentially across multiple locations.

The UK cannot achieve its desired aims by acting alone. However, the challenge posed by cross-border data storage is akin to the problem posed by tax-havens. There is likely to remain a number of storage locations around the globe that will remain profitable and desirable due to the regions disregard towards some international laws.

Areas of the internet will remain un-policable due to regional laws and policies, however even within compliant countries and regions, the internet many still be un-policable in cases were the data storage device simply cannot be located. Tor Hidden Services is the prime example. In this case data can be attributed to a specific hidden website, but the website cannot be attributed to a physical server as layers of effective encryption render the server "hidden". As such no legal seizure can be attempted until the server is discovered by some other means.

It is likely that such hidden services will remain, and will pose an international challenge even with 100% international buy-in and collaboration.

b. In the UK

The UK's data boarder is entirely porous. Data flows in and out of the UK freely. Any attempt to regulate the flow of data i.e. to block a certain file or a specific element of content is a fine grained level of control the UK does not possess. China has attempted such an engineering challenge and has had some success; however China's attempts, despite significant investment, are circumvented continuously by China's population.

Data boarders are unlikely to be achievable and the regulation of data in and out of the UK ultimately flawed. The UK possesses only course grained network level control. Many of the challenges posed to the UK as well as the rest of the world will reside at a higher level in the application layer. This is the layer in which China attempts to operate. The threat to privacy at this layer is massive, and effective control is only achievable through zero user privacy. This is a radical departure from the UKs current privacy position.

In the UK Communications Service Providers are likely to become increasingly marginalised with regards to information collection and control. Traffic and meta-data analysis will be the only available technology option. Again such approaches would require massive quantities of low value data to yield any value. It remains an open question as to how viable traffic analysis actually is when operated at such scale.

The change in delivery of Communication services over the past 15 years presents significant challenges to some of the base assumptions at the heart of both RIPA and related legislations such as Data Retention and Investigatory Powers Act (2014) (DRIP) and Anti-terrorism, Crime and Security Act (2001) (ATCSA). The key assumptions and questions that may have to be revisited are:

- Which organisation(s) generate and store data and therefore which types of organisations will future legislation need to apply to?
- Which communication services provided within UK will generate and store CD within the UK?
- What types of data are generated in the provision of communication services and therefore what can requesting agencies ask for?
- Is the existing definition of what constitutes a Communication Service Provider correct?

David Cole
Director
National Security Solutions
October 2014

Graham Smith

About the author

I am a solicitor in practice in London. My legal expertise is primarily in the fields of IT, the internet and intellectual property. I am the editor and main author of the textbook *Internet Law and Regulation*, first published in 1996 (4th edition 2007, Sweet & Maxwell).

I have advised private sector clients on RIPA from time to time since its inception. I contributed to the discussion of DRIPA during its rapid passage through Parliament, primarily through an analysis of the draft DRIP Bill posted on my Cyberleagle blog[1].

This submission is made in my personal capacity. It should not be taken as representing the view of any client for whom I have acted or of Bird & Bird LLP, the firm in which I am a partner.

Preliminary

This submission focuses mainly on paragraph (f) of the Review's Terms of Reference: the effectiveness of existing legislation. It is longer than I would have wished, mainly because a discussion of RIPA has to begin with the non-trivial exercise of decoding the statute. Hence some extensive supporting analysis, particularly of the external warrants regime.

My comments are structured as follows.

A. *Does anyone understand RIPA?*
B. *External warrants - the RIPA S.8(4) regime*
   - *Is S.8(4) a general warrant?*
   - *Capture, select, examine – the scheme of S.8(4)*
   - *Internal and external communications*
C. *Content and communications data*
D. *Judicial supervision*
E. *The broader impact of RIPA*
F. *DRIPA*
G. *Limits to investigatory powers*

Appendix: Diagram of warrants scheme

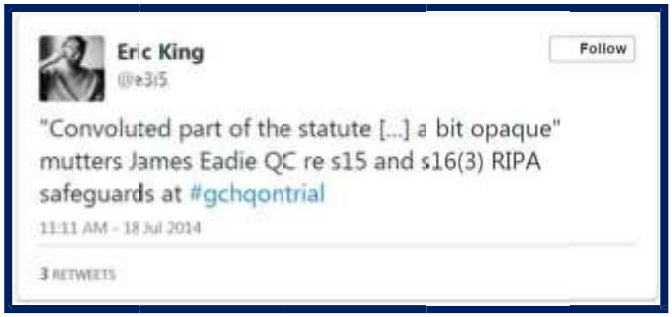
The Review will no doubt also be aware of the questions concerning S.94 of the Telecommunications Act 1984 raised by the Commons Home Affairs Select Committee in its Report on Counter-Terrorism (30 April 2014) at paragraphs 175 to 177.

1 http://cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html

A. Does anyone understand RIPA?

1. RIPA is a difficult piece of legislation:

> **2003**: "We have found RIPA to be a particularly puzzling statute" *R v W* (Court of Appeal)
>
> **2004**: "longer and even more perplexing" than the "short but difficult" IOCA 1985. Lord Bingham, *A-G's Ref (No 5 of 2002)*
>
> **2005**: "this impenetrable statute … one of the most complex and unsatisfactory statutes currently in force." Prof. David Ormerod ([2005] Criminal Law Review 220)
>
> **2006**: "a complex and difficult piece of legislation" Mummery L.J. (IPT/03/32/H)
>
> **2014**: "I do not think the ordinary person or Member of Parliament would be able to follow the Act without a lawyer…" Sir David Omand, former Director of GCHQ (evidence to Home Affairs Select Committee).
>
> **2014**: "RIPA 2000 is a difficult statute to understand" Sir Anthony May, IOCC Report 2013
>
> **2014**: The government's Q.C. in the TEMPORA and PRISM cases currently in the Investigatory Powers Tribunal, as reported from the hearing by a Privacy International live tweeter:



2. In short, the statute is obfuscated[2]. Whatever the appropriate reach and content of investigatory powers may be, that is unsatisfactory. Opacity is undesirable in any

[2] "In software development, obfuscation is the deliberate actof creating obfuscated code, i.e. source or machine code that is difficult for humans to understand." Wikipedia *Obfuscation (software)*. Whether or not the obfuscation of RIPA was deliberate, the result is not in doubt.

legislation, let alone a statute governing such significant matters as interception and access to communications data. It renders advising on RIPA, and indeed preparing submissions such as these, unnecessarily difficult. It makes for poor quality of law, in the sense of accessibility to those potentially affected by it.

3. The starting point for my comments is RIPA as drafted. To the extent that RIPA implements EU Directives they have to be taken into account, as does compliance with the ECHR and (to the extent relevant) the EU Charter of Fundamental Rights[3]. However, rather than attempt to read down specific RIPA provisions to align with often heavily debated EU law and ECHR constraints, I will for the most part take RIPA as it appears. If the drafting of RIPA creates tension with those external constraints, or if there is a significant gap between the drafting and more limited practice[4], that may be of concern to the Review.

B. External warrants - the RIPA S.8(4) regime

4. The Section 8(4) regime is currently under challenge in the Investigatory Powers Tribunal in the context of its hypothetical use to authorise GCHQ's TEMPORA programme.

5. The appended diagram illustrates the warrantry regime and the possible application of Section 8(4) to TEMPORA, partly informed by Charles Farr's witness statement in the IPT proceedings.

---

3 The interception offences in Section 1, although partially derived from the previous IOCA 1985 offence, also fulfil the UK's obligations to implement the confidentiality of communications provisions of (originally) the Telecommunications Data Protection and Privacy Directive (97/66/EC), followed by its successor Article 5(1) of the Electronic Communications and Privacy Directive (2002/58/EC). In May 2011 (S.I. 2011/1340) amendments were made to Section 1 and a new monetary penalty procedure introduced following a European Commission complaint that the Section 1 prohibitions did not correctly implement the Directive. (www.gov.uk/government/uploads/system/uploads/attachment_data/file/157979/ripa-amend- effect-lawful-incep.pdf). Article 15(1) of the EU Directive provides an exception from the Article 5(1) prohibitions applicable to interception for various specified purposes and subject to considerations of necessity, appropriateness and proportionality. At least the RIPA/DRIPA warrantry and mandatory retention of communications data regimes, to the extent that they apply to public services and networks as defined in the Directive, fall within this exception. Following the *Pfleger* decision of the CJEU (C–390/12 30 April 2014) it is likely that implementation of the Article 15(1) exception has to be compliant with the EU Charter of Fundamental Rights as well as with the terms of the exception and the ECHR.

4 *Cf* GCHQ's statement in 2009 as to its practice: "GCHQ does not target anyone indiscriminately - all our activities are proportionate to the threats against which we seek to guard and are subject to tests on those grounds by the Commissioners. The legislation also sets out the procedures for Ministers to authorise interception; GCHQ follows these meticulously. GCHQ only acts when it is necessary and proportionate to do so; GCHQ does not spy at will." (Reported in full at http://www.theregister.co.uk/Print/2009/05/05/gchq_mti_statement/.)

Is S.8(4) a general warrant?

6. A S.8(4) warrant authorises general[5], suspicionless capture of external and collaterally acquired internal communications. The captured communications can be trawled for indications of suspicious activity, not limited to persons of pre-existing interest[6].

7. The intended result of a Section 8(4) warrant is that suspicions (which may or may not turn out to be well founded) can be formed as a result of studying the fruits of the interception.

8. A section 8(4) warrant is therefore general in the sense that its *starting point* is broad, suspicionless capture of communications rather than targeted capture founded on specific pre-existing grounds. No amount of downstream safeguards can alter that.

9. In the IPT proceedings the government conceded that the capture stage engages the Article 8 privacy right:

> "… accept that the interception under a s.8(4) warrant may be regarded as giving rise to a technical interference [with ECHR Art 8 rights] even if that communication is not and/or cannot be read, looked at or listened to by any person."

10. On one view the only substantive interference with privacy rights occurs when a human being examines the material; and what really matters are the limitations and safeguards around that. On another view the possibility of surveillance is likely to give rise to a chilling effect[7].

11. We cannot know how Lord Camden might have reacted in *Entick v Carrington* had Lord Halifax said[8]:

> "Fear not, Mr Entick. True we have ransacked your home, broken the locks on your desks and cupboards and seized your papers and correspondence. But, since we have not yet examined any of them[9], that is a merely technical breach of privacy. We have strict safeguards in place to ensure that we will only look for material about that

---

5 The actual breadth of certificates is not disclosed. However RIPA permits broad descriptions. IOCC Report 2013 para 6.5.38: "a section 8(4) warrant permits the interception of generally described (but not indiscriminate) external communications."

6 The selection factors that can be used to trawl are limited by RIPA, particularly in relation to persons for the time being within the British Isles. The constraints are discussed below and are subject to exceptions. The extent (if any) to which analysts may be permitted to use material about persons within the British Isles that they may come across incidentally as the result of performing a search using other selection factors is also discussed.

7 E.g. JUSTICE "Freedom from Suspicion - Surveillance Reform for a Digital Age" October 2011, para 1; *Digital Rights Ireland* (C-293/12 and C-594/12) paras 27-28; Lord Neuberger "What's in a Name" 30 September 2014, para 31, in relation to confidential speech.

8 The parallel is not exact. All of Entick's papers were seized, not just correspondence. Entick was within the British Isles and was the focus of the warrant, whereas a Section 8(4) warrant captures mass external communications. Nonetheless, as we discuss, external communications include overseas communications to and from people within the British Isles; internal communications can be collaterally swept up; and the extent of protections for people within the British Isles is a topic for debate.

9 In fact the messengers did read some of the papers during the search.

renegade Wilkes who is skulking in Paris. Oh, if we happen to notice anything else of interest we can use it.[10]"

12. The ECJ in *Digital Rights Ireland* commented that blanket communications data retention under the Data Retention Directive did not offend against the essence of the privacy right because:

> "So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, *the directive does not permit the acquisition of knowledge of the content of the electronic communications as such*." (emphasis added)

13. S.8(4) does authorise general capture of content[11]. Its hypothetical application to TEMPORA reportedly involves a rolling 3 day content buffer as well as a 30 day metadata store.

14. As I discuss below, the precise ambit of RIPA's selection and examination provisions is not easy to discern. Even so, and putting on one side the special provisions of Section 16(3) and 16(5), it does appear that the Section 8(4) regime in principle could enable the relevant agencies to examine some internal communications and related communications data of persons known to be within the British Isles where no prior grounds for suspicion existed.

15. The most obvious scenario is where my internal communication[12] has responded as a 'hit' to a search conducted using a general selection factor or a factor referable to someone else outside the British Isles. The relevant agency can in principle examine my communication[13]. Whether it can then use the information to focus on me is less clear, as discussed below. What happens in practice is veiled in secrecy, albeit a corner of the veil has recently been lifted[14].

---

10 As discussed below it is not clear to this author whether incidental use is or is not possible under a S8(4) warrant, without making use of a special ground under S16 or an overlapping warrant..

11 These comments of the ECJ fall to be compared with the ECtHR admissibility decision in *Weber*, finding that the German government's 'strategic monitoring' programme was compatible with the Convention.

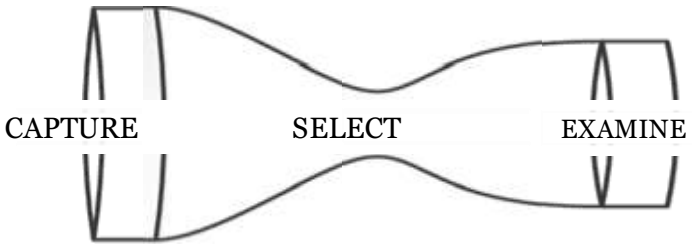
12 I.e. an internal communication captured collaterally to interception of external communications.

13 Although examination is limited to material described in the S8(4) warrant certificate, the certificate can be in general terms and need not be limited to external communications.

14 Charles Farr's IPT witness statement. Paragraphs 139 to 141 and 152 to 158 are the most relevant to this topic, emphasising that the practical focus is on external communications and stressing the purpose of Section 8(4): "But the primary purpose and object of any conduct authorised or required by a section 8(4) warrant must consist in the interception of external communications." (para 155).

Capture, select, examine – the scheme of S.8(4)

16. The overall scheme of the external warrants regime is hourglass-shaped, the width of the glass representing the degree of statutory constraint that applies at each stage[15].



17. C*apture* is constrained by the general purposes set out in RIPA S.5(3). Collateral capture of internal communications is empowered under RIPA S.8(5) and 5(6). However the primary purpose must be the capture of external communications.

18. Once captured, both internal and external communications are in principle available for examination, but subject to selection factor constraints.[16] The letter from Lord Bassam to Lord Phillips of 4 July 2000 during passage of the Bill, quoted below under 'Internal and external communications', stated *a propos* selection that "It would of course be unlawful to seek to catch internal communications…".[17] However the selection factor constraints themselves do not directly correspond to the distinction between internal and external communications[18].

19. *Selection* is categorised according to the selection factors under S.16(2), which determine how examination can and cannot be carried out.

20. The drafting is tortuous, but it seems clear that for examination to be *precluded* the selection factor must have triggered both limbs (a) *and* (b) of S.16(2).[19].

---

15 The width of the hourglass represents the constraints, not the volume of data at each stage.

16 See e.g. the government's Open Response in the IPT proceedings at page 47 (footnote 53).

17 http://www.fipr.org/rip/Bassam%20reply%20to%20Phillips%20on%20S.15.3.htm

18 But see para 139 of Mr Farr's witness statement: "Despite the fact that some UK to UK communications may be intercepted under section 8(4) warrants and that common uses of the internet by persons in the British Islands, such as a Google search, a Facebook post, or a "tweet" on Twitter, may entail the making of "external communications" for the purposes of Chapter I of RIPA, the section 8(4) regime as a whole is designed so as not to authorise the selection for examination of communications of this nature, except in the tightly constrained circumstances set out in section 16 of RIPA. It is therefore unlikely that such communications would be capable of being read, looked at or listened to, even in the unlikely event (see paragraph 157 below) that they fell within a description of communications to which a section 8(4) warrant related." However it is not clear from paragraph 157 why such communications would be unlikely to fall within the description in a certificate.

19 This is supported by the language of S.16(3): "any such factor [*singular*] as is mentioned in paragraph (a) *and* (b) of that subsection". See also para 5.12 of the draft revised Interception of Communications Code of Practice: "Where the requirements of section 16(3) of the Act are m t, the certificate may be modified to authorise the selection of communications sent or received outside the British Islands according to a factor which is referable to an individual who is known for the time being to be in the British Islands *and* which has as its purpose, or one of its purposes, the

21. S.16(2) appears to have the effect that examination is *permissible* if:
    1. Selection was by means of a general factor not referable to any individual (such as the search term 'Syria' or 'Semtex').
    2. Selection was according to a factor referable to an individual known for the time being to be outside the British Isles.
        - So my name could be used as a search term if I am known for the time being[20] to be outside the British Isles[21].
    3. Selection was according to a factor referable to an individual inside the British Isles if it did not have as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.
        - So if it were thought that I might be mentioned in e-mails of someone outside the British Isles[22], my name could be used as a search term to identify that person's e-mails to people other than myself, even though I am known to be within the British Isles.
        - Apparently[23], that could also be done if a purpose of using my name as a selection factor was to identify e-mails between the target person and other people known to be within the British Isles (assuming that the selection factor - my name - is not 'referable to'[24] those people).
    4. Selection was according to a factor referable to an individual whose location was unknown. This seems to be the effect of S.16(2) taken alone. On the other hand the S.16(6)(b) defence might appear to presuppose a positive belief that the individual is outside the British Isles.

22. The scope of permissible examination thus seems to be wider than might be thought from reading Lord Bassam's statement at Col 323 of Hansard 12 July 2000, which reflects only S.16(2)(a):

> "selection may not use factors which are referable to an individual known to be for the time being in the British Islands"

---

identification of material contained in communications sent by him or intended for him." (emphasis added.)

[20] This appears to refer to the time of the selection, not the time of sending or receiving the communication. If so, this is a significant difference from the internal/external communications distinction. I could send an internal communication today and go abroad tomorrow. While I am abroad my name could be used as a selection factor to identify and examine that internal communication.

[21] Paragraph 195.3 of the government's Open Response in the IPT proceedings states "Thus, by way of example, intercepted material could not in general be selected to be listened to by reference to a UK telephone number." However would that apply if the UK telephone number in question was of a mobile phone and the owner was known for the time being to be outside the British Isles?

[22] I have assumed that use of my name to identify e-mails of someone else within the British Isles could be use of a factor referable to that person. "Referable to" is not defined in RIPA, but I would assume to be broader than identifying.

[23] But could this amount to unlawfully seeking internal communications? (see Lord Bassam's letter to Lord Phillips of 4 July 2000.) There may be tension between what is apparently permitted by the wording of S16(2) and the limiting overall purpose of S.8(4) (interception of external communications) (which itself should be viewed in the light of Articles 5(1) and 15(1) of the EU Privacy and Electronic Communications Directive 2002/58/EC)

[24] If my name is a selection factor referable not only to me but to my associates, it is still difficult to see how that could include associates of the target person who are not known to me.

23. The statutory references to selection factors map well on to automated filtering by the use of search terms and keyword or similar searches made manually by analysts. The draft revised Interception Code published in 2010 recognises (paragraphs 6.5 and 6.6) that selection factor constraints apply both to automated filtering and to subsequent selection factors applied manually by analysts.

24. *Examination* is subject to the general RIPA purposes and the description of materials in the warrant (which it appears can be very broad – e.g. all communications with a named country). Examination is not of itself subject to the restrictions on selection factors or limited to external communications.

25. However is an analyst who reviews material produced as the result of searches simultaneously examining and continuing to select?

26. The Interception Commissioner's Report 2013 at paragraph 6.6.15 refers to "examination by a person upon specific individualised inquiry". Assuming that 'specific individualised inquiry' forms part of the selection stage, it is not obvious whether (and if so when) there comes a point at which selection ceases and only (less constrained) examination of the previously selected corpus of material is taking place.

27. What therefore is the position where an analyst becomes incidentally aware, while examining appropriately selected interception product, of material thought to be of interest concerning someone known to be within the British Isles?

    - If the material is a wholly third party communication, then even if the selection factor constraints still apply they would appear not to prevent the examination and use of the material within the general statutory purposes and the S8(4) certificate (since S.16(2)(b) would not be triggered).

    - If the material is a communication sent by or intended for that person, then to focus on it would potentially breach the selection factor constraints, but only if they are still applicable at this stage.

28. It is not obvious whether in such cases the use of such incidental material is permissible, or if it can be examined only under S.16(3), 16(5)(a), or (apparently[25]) if an overlapping S8(1) warrant is in existence.[26].

---

[25] The continued use of overlapping warrants was confirmed by Lord Bassam in the extract from the 12 July 2000 Hansard footnoted by the Interception Commissioner at paragraph 6.3.68 of his 2013 Report: "Beyond that are the safeguards set out in subsection (2) of Clause 15. Except in the special circumstances set out in later subsections, or if there is an "overlapping" Clause 8(1) warrant, selection may not use factors which are referable to an individual known to be for the time being in the British Islands.". The Interception Commissioner's 2013 Report makes no other mention of overlapping warrants.

[26] Overlapping warrants were first described in the Interception Commissioner's Report for 1986 under IOCA (March 1987, para 36). It appears that their purpose is to buttress the legitimacy of examining communications to or from persons within the British Isles legitimately made available through the Section 8(4) selection procedure. This Review presents an opportunity to re-examine and clarify the purpose and use of this practice.

29. The explanation in the Interception Commissioner's 2013 Report at paragraph 6.5.35 corresponds to S16(2)(a), applying the British Isles restriction to *selection*[27]. Paragraph 6.5.34 goes further however, stating that it relates to *examination*. This could perhaps reflect an understanding that examination necessarily entails continuing selection.

30. In the next section I suggest that the Interception Commissioner's Reports could usefully contain explanations of legal interpretations on the basis of which intelligence agencies are operating. The issues discussed in this section are an example of where this would be helpful.

Internal and external communications

31. An external communication is one "sent or received outside the British Islands". On this short phrase rests the entire foundation of Section 8(4) warrants (see RIPA S. 8(5)(a)).

32. RIPA S.8(5)(b) and 5(6)(a) empower the collateral capture of internal communications. Lord Bassam, in his letter to Lord Phillips of 4 July 2000, said:

> "…in some cases selection will unavoidably be applied to all intercepted communications. This selection is in practice designed to collect external communications that fit the descriptions in the certificate. It is therefore not likely to catch many internal communications. It would of course be unlawful to seek to catch internal communications in the absence of an overlapping warrant or a certificate complying with clause 15(3)"

33. The Interception Commissioner's Report for 2013 says at 6.5.54:

> "…my investigations indicate that the volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications and of the total available to an interception agency under a section 8(4) warrant."

34. Subsequently the Home Office's particular interpretation of "external communication" (discussed below) has been revealed in the current IPT proceedings.

35. Overall the situation is problematic:
    - The interpretation of the critical phrase 'external communication' adopted by the Home Office is controversial (an interpretation that would probably never have emerged but for the IPT challenges arising from the Snowden disclosures).
    - In many situations the intercepting authorities cannot know whether what they are intercepting under a S.8(4) warrant is an internal or external communication.
    - The significance of the distinction between internal and external communications is potentially weakened by the power collaterally to sweep up internal communications (S. 8(5)(b) and 5(6)).

---

[27] This is also the position set out in paragraph 6.3.38 of the Report and by Lord Bassam in the extract from Hansard footnoted in that paragraph.

- If the Home Office interpretation presented in the IPT proceedings is correct in law, then the already problematic distinction between internal and external communications is further undermined.

36. Identifying these problems is not to say that the use of S8(4) warrants is now unconstrained by the distinction. So it is difficult to see how a S8(4) warrant could be used to intercept on a communications link running between points within the British Isles, assuming no ability to separate external from internal communications.

37. Turning to what is and is not an external communication, in a fixed landline system it should be simple enough to determine where a communication is sent or received. However that becomes more difficult as we introduce cumulative factors such as:
    1. Mobility
        (i) whether a mobile phone call is internal or external depends on the happenstance of where the parties are located when the call is made
    2. Stored one to one (or one to few) server-based communications such as voicemail and e-mail
        (i) is the communication received by the intended human recipient
            - at the server?, or
            - at the location of the intended human recipient?
        (ii) If at the location of the intended human recipient, is that his or her location:
            - when the communication is available to be picked up?
            - when it is received on the human recipient's device?
            - when the human recipient opens it on the device?
    3. Communications with corporate entities
        (i) Can a corporate entity be an intended recipient for the purposes of RIPA?
        (ii) If so, does a corporate entity send or receive a communication at its place of business, its place of incorporation, the location of its server or data centre, or (e.g. if its data are spread dynamically across geographically distributed data centres) the location of a gateway to its internal network?
    4. One to many communications. Does the fact that the sender cannot be sure of the identity of some or all of the recipients change the analysis? e.g.
        (i) An e-mail mailing list managed by someone else. Is the intended recipient(s) the members of the mailing list at the time of sending the communication, the manager of the mailing list or the server via which the communication is distributed to the members of the mailing list is distributed?
        (ii) A social media platform. Are the intended recipient(s) the potential readers of the post or tweet? Or is it the platform (and if so, is it the server or the entity operating it)?

38. As illustrated by Mr Farr's IPT witness statement, the answers to these questions crucially affect whether significant categories of communications are internal or external. His key points are:

E-mail

> *"129 … the relevant question to ask is not via whom (or what) a message has been transmitted, but for whom (or what), objectively speaking, the message is intended.*

Thus, an email from a person in London to a person in Birmingham will be an intemal not external, communication for the purposes of RIP A and the Code, whether or not it is routed via IP addresses outside the British Islands, because the intended recipient is within the British Islands. The intended recipient is not any of the servers that handle the communication whilst en route (whether that server be located inside, or outside, the British Islands). Indeed, the sender of the email cannot possibly know at the time of sending (and is highly unlikely to have any interest in) how that email is routed, or what servers will handle it on its way to the intended recipient."

39. This addresses point 2(i) above. It adopts the same reasoning as for mobile telephony, in that the locations of the intended human sender and recipient are determinative.

40. Mr Farr does not address point 2(ii). This issue can be illustrated by text messages.

41. Consider a text message sent from the British Isles to someone in flight from USA to the British Isles while the phone is switched off. The message is stored at the phone provider within the British Isles and picked up by the phone when it is activated upon arrival in the British Isles. The phone's user then opens the message. Is that an internal or external communication? Was the communication received when it was available for collection, or when it was picked up by the device (or when opened)? Does the location of receipt depend on the location of the recipient at the relevant time, or on the location of the phone company facility at which it was stored for later collection by the recipient?

42. What if the recipient had left the telephone in the British Isles (switched on), so that the text message was picked up by the phone in the British Isles while the recipient was out of the country? Is that internal or external?

43. Mobile telephone calls, e-mail, voicemail and text messages are all examples of situations in which, if the interception is effected between the sender and the provider, the intercepting authority cannot know whether the communication is internal or external. It cannot know whether the human recipient (or, if relevant, the mobile device itself) is within or outside the British Isles at the relevant time (whenever that may be)[28].

Search request and response

"133. A person conducting a Google search for a particular search term in effect sends a message to Google asking Google to search its index of web pages. The message is a communication between the searcher's computer and a Google web server (as the intended recipient). The Google web server will search Google's index of web pages for search results, and in turn send a second communication - containing those results - back to the searcher's computer (as the intended recipient).

---

[28] This was understood at the time of the Bill. Lord Bassam, Hansard, 12 July 2000: "Even after interception, it may not be practicably possible to guarantee to filter out all internal messages. Messages may well be split into separate parts which are sent by different routes. Only some of these will contain the originator and the intended final recipient. Without this information it will not be possible to distinguish internal messages from external. *In some cases it may not be possible even if this information is available. For example, a message between two foreign registered mobile phones, if both happened to be roaming in the UK, would be an internal communication, but there would be nothing in the message to indicate that.*" (emphasis added)

134. Google' s data centres, containing its servers, are located around the world; but its largest centres are in the United States, and its largest European centres are outside the British Islands. So a Google search by an individual located in the UK may well involve a communication from the searcher's computer to a Google web server, which is received outside the British Islands; and a communication from Google to the searcher's computer, which is sent outside the British Islands. In such a case, the search would correspondingly involve two "external communications" for the purposes of section 20 of RIPA and paragraph 5.1 of the Code."

44. This touches on points 3(i) and (ii) above. Mr Farr starts by suggesting that the message is to Google, but then suggests that the intended recipient of the search request is not Google the entity but Google's web server. He then goes on to suggest that the intended recipient of the response is not the searcher, but the searcher's computer. Why the position should be any different from e-mail, where he appears to accept that the recipient is the human being not the device, is not explained.

Social media

"136. Making a post on Facebook, or "tweeting" on Twitter, entails placing a message upon a web-based platform, in order that it can be seen by a wide audience. In such a case, the recipient of the relevant "communication" is not any particular person who eventually reads the post or tweet, whose exact identity the person posting or tweeting cannot possibly know at the time the message is sent. Rather, it is the platform itself, because the platform is both the repository for the message, and the means by which it is broadcast to those with access to the relevant Twitter account or Facebook page.

137. Thus a user located in the British Islands posting a message on Facebook will communicate with a Facebook web server, located in a Facebook data centre. If the Facebook data centre is outside the British Islands, then the message will be an "external communication". (It is also possible to use Facebook to send an email to an individual: and in such a case, the recipient of the communication would be that individual himself; and - as in the case of other types of email - whether or not the communication was internal or external would depend upon where that individual was located but not on how the email was routed.)

138. Similarly, a user located in the British Islands posting a message on Twitter will communicate with a Twitter web server forming part of Twitter's data centre infrastructure. That data centre infrastructure is largely based in the United States; so the communication may well be "external' for the purposes of RIP A and the Code."

45. This addresses point 4(ii) above. Unlike with the search engine example Mr Farr is not explicit that the data centre (as opposed to the entity controlling it) is the intended recipient. However he is clear that he regards the location of the data centre (not the location of the entity that controls it) as determining the place of receipt.

46. Mr Farr does not address point 4(i), nor offer any explanation as to why his interpretation is to be preferred to one whereby the potential readers of the tweet or post are the intended recipients.

47. Summarised, his position appears to be as follows:

	Email	**Google search (request)**	**Google search (response)**	**Facebook/Twitter**
Sender	Human sender	Human user?	Google server (not Google the entity)	Human user
Intended recipient	Human recipient	Google server (not Google the entity)	Human user's computer (not the human user)	Facebook/Twitter server (not the entity)

48. It is difficult to discern from this a consistent principle as to when the place of receipt should be determined by the location of a server and when by the location of a person (whether human or corporate entity), nor as to when (and why) the intended recipient is the human being, the corporate entity or the device.

49. These questions, insofar as they stray into consideration of who is the sender and intended recipient, have implications beyond the distinction between internal and external communications under Section 8(4). Much of RIPA contemplates that sender and intended recipient are persons (natural or possibly corporate[29]), not devices[30].

50. Mr Farr's statement provoked controversy when it was published. If we assume that a British subscriber to Facebook or Twitter will typically number other persons located within the British Isles among his or her friends or followers, Mr Farr's interpretation converts a very large number of what would otherwise be internal communications into external communications.

---

[29] See the author's *Internet Law and Regulation* (Sweet and Maxwell, 4th Edition) Chapter 5 pages 418 to 422. We have to remember that as well as providing a human rights compliant interception regime RIPA (through the S.1 interception offence) implemented Article 5 of the then Telecommunications Data Protection and Privacy Directive (97/66/EC). This required Member States to "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than *users*, without the *consent of the users concerned*, except when legally authorised, in accordance with Article 14 (1)." (emphasis added.) RIPA translates users (presumptively able to give consent) into senders and intended recipients. A device (including a server) is not a user and cannot give consent. Its operator can do so, via the device or separately.

[30] S1(3) assumes that the sender, recipient or intended recipient is someone capable of taking legal action: "shall be actionable at the suit or instance of the sender or recipient, or intended recipient"
S3(1) presupposes that the sender or intended recipient is capable of giving consent:
"(a) a communication sent by a person who has consented to the interception; and
(b) a communication the intended recipient of which has so consented."
Similarly S3(1): "a communication the intended recipient of which has so consented."
and S3(2(a): "the communication is one sent by, or intended for, a person who has consented to the interception"
S48(4)(a) "the communication is one sent by or intended for a person who has consented to the interception of communications sent by or to him;"
The definition of "communication" in S.81(1)(c) includes communications between 'things'. However it does not necessarily follow that a sender or intended recipient can be a thing. A person can send a communication from a thing or receive it at a thing. Everyday internet communications include many messages sent to and from respective devices which are not directly initiated by the user and of which the user is not aware. The user can still be the sender or recipient of those messages and be capable of giving consent in relation to them. If the device is the sender or intended recipient, that is not possible.

51. If Mr Farr's interpretation is wrong in law, then the government may have been operating on the basis of flawed interpretations of RIPA. If it is right, the already fragile distinction between internal and external communications is weakened.

52. It is unclear to what extent the government has operated on the basis of these interpretations in the past. The IOCC Report for 2013 stated:

> "in any event my investigations indicate that the volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications *and of the total available to an interception agency under a section 8(4) warrant*." (emphasis added)

53. The Report does not set out any particular interpretation of RIPA on which that evaluation was founded.

54. It would be a significant advance if future IOCC Reports were to set out in the non-confidential section the legal interpretations of investigatory powers legislation on the basis of which the relevant agencies and authorities have been operating.

C. Content and communications data

55. The richness of communications data has increased dramatically since the days of telephone numbers, call duration and subscriber lookups. Communications data now form a rolling map of our lives. General capture or mandated retention of mass communications data (with or without content) is very close to posting an intelligence agency bot in the living room.

56. The old assumption that communications data is inherently less sensitive than content no longer holds good. Communications data can be as revealing as content – even taking into account the statutory limitations that treat anything after the first slash of a URL as content – or more so. The mantra "It's only metadata" is no longer sustainable.

57. The reality was brought home vividly in a New York Review of Books article by Paul Cole in May this year:

> "As NSA General Counsel Stewart Baker has said, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct," and raised him one, asserting, "We kill people based on metadata."[31]

58. Content, it should be stressed, has not become any less sensitive. Communications data has become more so.

---

31 www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/

59. Communications data is an area that is ripe for reassessment. The very richness and mobile trackability that renders it so attractively useful for law enforcement and intelligence agencies commensurately increases the impact on privacy when it is retained, captured and accessed. Comparisons with even a few years ago are now of little value.

60. Some more specific concerns with communications data relate to privilege[32] and the position of related communications data captured under S8(4) warrants.

61. The relatively fewer restrictions on the use of related communications data captured under an interception warrant is an issue in the IPT proceedings. It is reported that under TEMPORA communications data are held for 30 days.

62. Various points discussed in the Communications Data Bill Joint Committee Report in December 2012 remain live issues, although some have been superseded by DRIPA. These include the list of authorities and statutory purposes, the question of a capability gap (and whether CSPs should be required actively to generate certain data), the definitions of communications data (do they cover too much data or too little?), blurring of distinctions between content and communications data (for instance communications taking place within virtual world or game environments) and whether to future-proof or take one step at a time. As to that, the risk of unintended privacy-invasive consequences as technology evolves is greater if a technology-neutral approach is adopted[33].

D. Judicial supervision

63. Lack of judicial involvement in the issue of warrants and communications data notices has always been controversial. Judicial supervision by magistrates has been introduced for communications data notices issued by local authorities.

64. The ECJ in the *Digital Rights Ireland* case stated as one reason for invalidating the Data Retention Directive that:

> "Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions." [62]

---

[32] The government has indicated that the Communications Data Code of Practice will be amended to take into account privilege concerns, following the *Digital Rights Ireland* case. The recent publicity regarding cases of identification of journalist sources has focused attention on this aspect. Since journalistic privilege is strongly rooted in protection of the *identity* of sources (see e.g. *Financial Times v UK* Case 821/03, paragraphs 60 to 63), acquisition of communications data capable of revealing a source would seem to engage journalistic privilege as directly as access to content. But see the Interception Commissioner's statement of 4th September 2014.

[33] See e.g. Escudero-Pascual, A. and Hosein, I. (2002), "The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data", Communications of the ACM, Volume 47, ISS3, (April 2004). Available at: http://doi.acm.org/10.1145/971617.971619.

65. Add to this the Snowden revelations about the extent of general data capture under TEMPORA and there is a strong case for revisiting the question of prior judicial authorisation of both interception warrants and communications data acquisition notices and authorisations.

E. The broader impact of RIPA

66. Whilst the broader impact of RIPA may be outside the strict remit of the Review, changes to RIPA have consequences beyond the warrantry and communications data acquisition regimes.

67. The same definition of interception applies to the interception offence, the civil liability provisions and the warrantry provisions.

68. The rationale for the interception offence was at least partly to implement the communications confidentiality provisions of (originally) the Telecommunications Data Protection and Privacy Directive (97/66/EC). Its successor is the Electronic Communications and Privacy Directive (2002/58/EC). Interception falls under the Article 15(1) exception. The Lawful Business Practice Regulations also implement exceptions permitted under that Directive.

69. Since warrants cannot authorise activity that does not amount to an interception, the courts may tend to interpret interception broadly so as to avoid prejudicing the warrantry regime. However the consequence of that could be that activities by non-State actors, which may amount to interception only in the most technical sense, may fall foul of RIPA Section 1 prohibitions. That in turn could result in a prohibition of broader scope than required by the Directive.

70. A point that can give rise to particular difficulty is the S2(2)) definition of interception, requiring that monitoring etc be such:

> "as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication"

71. The simple case is someone listening in to a call via a tap. Or if a device attached to the telephony equipment records the call for someone to listen to later that is caught by S2(8).

72. But what if the process is entirely computerised, automated and transient, without revealing the contents of the communication to a human being or recording its contents for later human appraisal?

73. No human being has read or will read the contents of the communication. But does a 'person' for this purpose have to be a human being? If a computer (under the control of some organisation) has scanned, parsed and analysed the communication on the fly is

that sufficient to be an interception? If so[34], then something akin to pure monitoring falls within the definition. If not, then (since a warrant can only authorise an interception) there would be no statutory basis on which a warrant could authorise what would seem to be a privacy-engaging activity by the State.

74. Questions have been raised whether ISPs' blocking of child pornography, spam or specific website locations could amount to an interception under RIPA, and if so whether that is authorised under (for instance) Section 3(3)[35].

75. What should and should not amount to interception for the purposes of (a) the S.1/EU Directive prohibitions and (b) the warrantry regime may be a topic for future consideration.

F. DRIPA

76. The DRIPA amendments affect:
    (a) The providers who can be required to retain data (*viz* the change from EU-based definitions of services to the newly amended RIPA definitions[36])
    (b) The providers who can be required to intercept or to provide communications data (*viz* the amendment to the RIPA definition of telecommunications services)
    (c) The territorial location of the conduct that can be required by an interception warrant or a communications data notice (*viz* the amendment to RIPA explicitly to include conduct outside the UK)
    (d) The ability to serve warrants and give communications data notices to non-UK service providers (*viz* the new, elaborate service provisions)

77. It is difficult to test the proposition that DRIPA amendments only clarify and do not extend RIPA. We do not know the baseline for comparison. Is it what the Home Office thought in 2000? Is what the Home Office has subsequently decided is a reasonable or possible interpretation of RIPA? Is it what the Home Office intended or hoped RIPA would cover and has now realised it may not? Is it the practice that has been adopted under RIPA? If so, has that been uniform over time?

78. The government's TRIS notification to the European Commission[37] stated:

---

34 The example given by Lord Bassam at Hansard 12 June 2000 Col. 1437 may support the interpretation that mere automated scanning amounts to an interception, since his comments suggest that an interception has taken place without any human being looking at the screen. But paras 8 and 9 of the informal Home Office note here (http://cryptome.org/ho-phorm.htm), which became public in January 2008, may suggest room for differing opinions.

35 See for instance www.ispreview.co.uk/index.php/2014/03/uk-online-safety-report-finds-isp- website-blocks-unsuitable-tackling-porn.html

36 The fact that part of the purpose of RIPA was to implement (originally) the Telecommunications Data Protection and Privacy Directive (97/66/EC) means that so far as possible the courts should interpret the RIPA definitions relating to public telecommunications services and systems consistently with the UK's implementation obligations. The RIPA definitions ought therefore not to be narrower than those in the Directive. However the UK may adopt legislation with a broader scope than that of the Directive (or its successor).

37 http://ec.europa.eu/enterprise/tris/en/search/?trisaction=search.detail&year=2014&num=354

> "The legislation clarifies existing provisions of the Regulation of Investigatory Powers Act which were previously notified to the Commission (2000/0069/UK). This is, in part, to react to domestic case law which may lead to Act being interpreted in a more limited way than when the Bill was passed and the Act notified." (The reference to domestic caselaw is not elaborated.)

79. Consider the territoriality amendments. The interception offence in Section 1 RIPA is explicitly limited to interception 'at any place in the United Kingdom'. S.2(4) explains what interception 'in the United Kingdom' means for the purposes of the Act. However, nowhere else in the Act is (or was) anything made dependent on interception being effected at a place in the United Kingdom.

80. The pre-DRIPA warrantry provisions, in particular, were not on their face limited to an interception in the United Kingdom. Even pre-DRIPA therefore, a warrant served within the UK was unconstrained by any explicit statutory territorial restriction on the location of the required interception. DRIPA now makes the possibility of requiring extra-territorial conduct explicit, makes explicit that non-UK providers can be subject to the relevant duties and also provides methods for serving non-UK entities within the UK.

81. The Interception Commissioner's 2013 Report states at paragraph 2.4:

> "My statutory role concerns interception within the United Kingdom."

82. That describes the territorial scope of the S.1 interception offence. However it does not seem to reflect any lack of territorial constraint on the place of interception in the warrantry provisions.

83. So what was the pre-DRIPA baseline? Was it interception limited to conduct within the UK, or did it include (as now clarified by DRIPA) conduct outside the UK?

84. The question of whether the data retention aspects of DRIPA comply with either the Human Rights Act or the EU Charter of Fundamental Rights will no doubt be tested in court on some future occasion.

85. The investigatory powers aspects of DRIPA raise some issues.

- The supplemented definition of 'telecommunications services' does on the face of it appear to be wider than the original definition.

86. This stems from:

    a. the omission in the supplemental definition of "access to" and "facilities for making use of" a telecommunications system.

b. use of the term 'facilitating' (much broader than 'provision') 'the creation, management or storage of communications transmitted, or that may be transmitted, by means of' a telecommunications system.

c. is a communication that 'may be transmitted' essentially a document stored in a connected environment?

87. Even if there might be room for debate about whether in practice these amendments do or do not catch more real world services than before, the wording is wider than before.

- The new RIPA S11(5A) introduces consideration of conflict with the law of the country in which the steps are required to be taken. It applies only to non-UK operators.

88. This is limited to non-UK operators. However a UK operator required to take steps in another country could face the same issue. It produces the curious result that a UK operator required to implement an interception in country X would not be able to invoke the provision. But a German operator could do so, even though country X is not its home country.

89. No similar provision is introduced for communications data notices. It is unclear why not, since a conflict with foreign local law could equally well arise.

G. Limits to investigatory powers

90. The human rights compatibility of investigatory powers brings into play quality of law, necessity for a legitimate purpose, proportionality and (per Article 52 of the EU Charter of Fundamental Rights) the essence of the right or freedom. Some State powers may be so intrusive or offensive as to be off limits, however useful and convenient they may seem, however strict the controls over their exercise and however stringent the safeguards over the use of their fruits.

91. State surveillance of communications goes to the heart of the relationship between citizen[38] and State. Hogan J. in the recent High Court of Ireland case of *Schrems*[39] said:

> *"By safeguarding the inviolability of the dwelling, Article 40.5 provides yet a further example of a leitmotif which suffuses the entire constitutional order, namely, that the State exists to serve the individual and society and not the other way around."*

92. He went on:

---

[38] Under RIPA and DRIPA the communications data retention and acquisition provisions apply generally regardless of citizenship. The S.8(4) provisions for interception of external communications (content and related communications data) affect UK as well as non-UK citizens, notwithstanding the various restrictions based on presence for the time being within the British Isles. I will use 'citizen' in the broad sense of those within the umbrella of a State.

[39] *Schrems -v- Data Protection Commissioner* [2014] IEHC 310 (18 June 2014)

"In this regard, it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home - such as e-mails, text messages, internet usage and telephone calls - would pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation."[40]

93. Former Defence Secretary Liam Fox provided a different view. He was reported in June this year as saying:

"The whole area of intercept needs to be looked at," ... "We have got a real debate, and it is a genuine debate in a democracy, between the libertarians who say the state must not get too powerful and pretty much the rest of us who say the state must protect itself."

94. The primary purpose of investigatory powers is, or ought to be, protection of the citizen. However a duty to protect citizens does not entitle the State to post a policeman in every living room for the protection of the occupants.

95. Still less is the State entitled to do that in pursuit of its own interests. If the point of departure is the State's interest in protecting itself, the destination is liable to be a regime weighted in favour of State powers and routine intrusion.

96. The interests of the State and the interests of citizens are not presumptively aligned. They may well be opposed to each other. Fundamental rights at their core perform the necessary function of protecting individuals from their own State. State demands for powers to access communications should be evaluated against that backdrop.

97. States have always had a propensity to claim broad powers on grounds of necessity, convenience, usefulness and the greater good. In 1765 counsel for the defendant King's Messengers in *Entick v Carrington* argued, unsuccessfully:

"Supposing the practice of granting warrants to search for libels against the state be admitted to be an evil in particular cases, yet to let such libellers escape, who endeavour to raise rebellion, is a greater evil..."

98. By 1765 the practice of issuing general warrants had been established for some 80 years, considerably longer than present day government programmes for broad capture of electronic communications. Counsel for the King's Messengers argued:

"I am not at all alarmed, if this power is established to be in the secretaries of state. It has been used in the best of times, often since the Revolution."[41]

Counsel for Entick responded:

---

[40] Others reject the notion that capture equates to access, and would argue that the potential for abuse can adequately be mitigated by downstream safeguards. See discussion of RIPA Section 8(4) above.

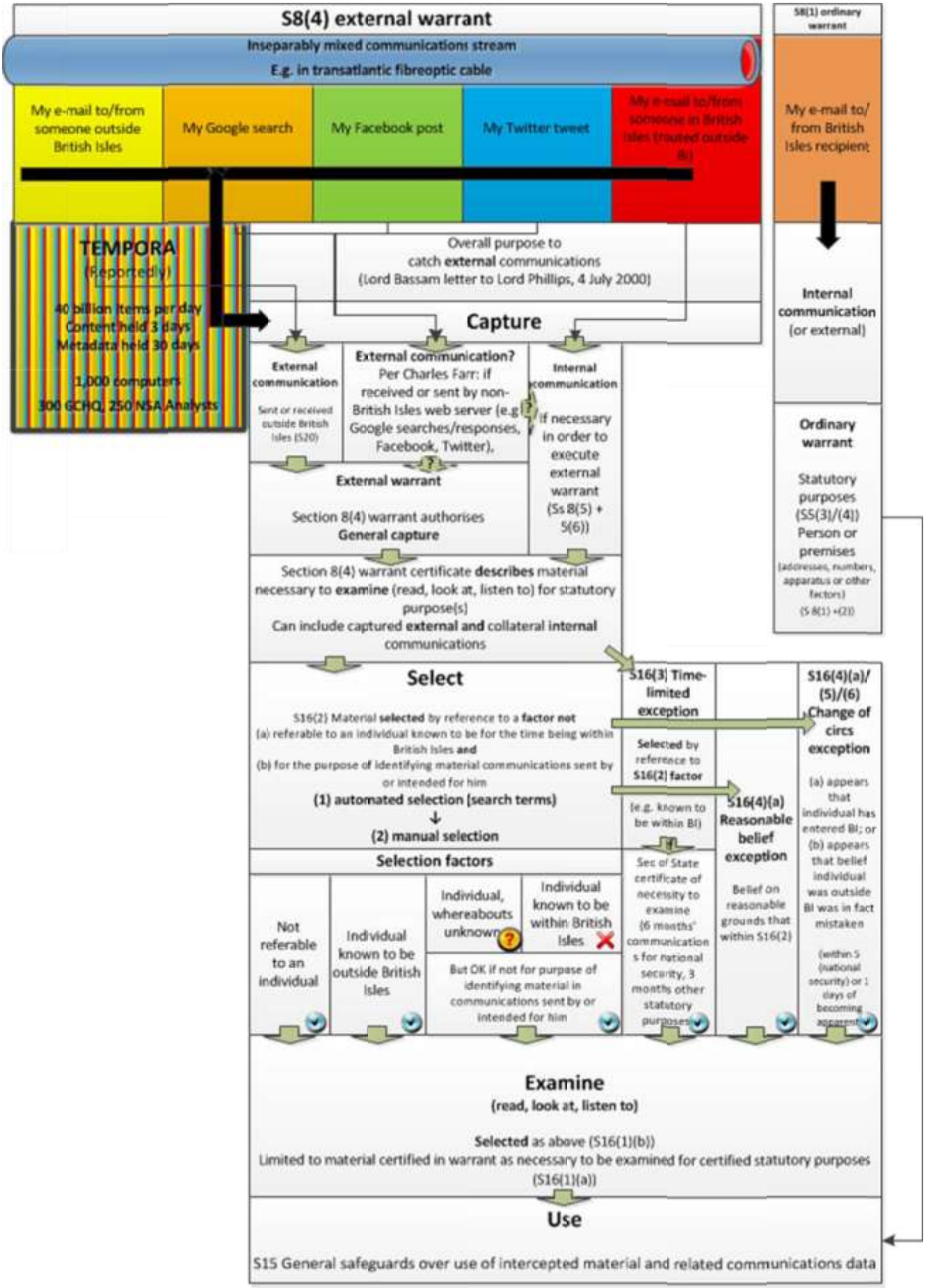
[41] The Glorious Revolution of 1688.

"It is said, this has been done in the best of times ever since the Revolution. The conclusion from thence is, that it is the more inexcusable, because done in the best of times, in an era when the common law (which had been trampled under the foot of arbitrary power) was revived."

99. 80 years of usage did not deter Lord Camden from striking down the practice of issuing general warrants. Nor should we shrink from challenging an established modern practice if it is so intrusive as to be off limits.

October 2014

Appendix: Diagram of Warrants scheme



Society of Editors

I am writing to confirm the Society's support for comments you will have received from the Newspaper Society, the Media Lawyers Association and a range of other bodies regarding concerns about the current operation of the Act.

The Newspaper Society, Society of Editors and broadcasting companies made representations during the passage of RIPA Bill and thereafter on the necessity for better protection of journalistic sources. We drew attention, for example, to the specific safeguards for confidential journalistic sources and material in PACE, the Police Act and the Data Protection Act as well as under the general law. We also supported enhanced transparency and better public oversight of the functioning of the system.

As you are aware this has been the subject of considerable reporting and comment of late and we have written to the Prime Minister about our renewed concerns. I am attaching a copy of that letter for you information.

The Society of Editors has more than 400 members in national, regional and local newspapers, magazines, broadcasting and digital media, journalism education and media law. It campaigns for media freedom, self regulation, the public's right to know and the maintenance of standards in journalism. We would certainly support changes to the primary legislation which would provide better protection to confidential journalistic sources their lawful investigation and report on local, regional, national and international matters.

Bob Satchwell
Executive Director
October 2014

The Right Hon David Cameron MP Prime Minister
10 Downing Street London
SW1A 2AA

Dear Prime Minister,

The Society of Editors is extremely concerned about the use of the Regulation of Investigatory Powers Act to check on journalists' phone records. This rides roughshod over protections for journalists' sources in other legislation and protocols that are frequently upheld by the courts – and indeed endorsed by politicians.

When RIPA was enacted we were told it was intended to help fight terrorism and, understandably, major crime, such as drugs and people trafficking, organised and economic crime.

Clearly the use of RIPA in this way has implications that extend far wider than the vital role of journalism in society, to the public generally and indeed for Parliament that enacted the legislation.

At a time when Ministers point to a reduction in crime, the latest figures which reveal a widespread use of this powerful but supposedly restricted weapon to access phone records mean that either politicians are being misled or the police are applying an extremely loose interpretation of "major crime" or indeed national security.

The Metropolitan Police is reported to have used RIPA 95,000 times in a year to access phone records. It also seems surprising that police in rural Norfolk and Suffolk should have used RIPA 4,000 times over two years.

According to Press Gazette more than 25 police forces have refused to provide details under the Freedom of Information Act, some saying it would cost too much to find the information. Others have used the excuse of protecting "national security" or the need to protect their tactics from criminals. In the two matters which have made headlines, the so-called "Plebgate" affair and the Huhne speeding points case, journalists were targeted without any apparent suggestion of criminality on their part or that national security was involved. There appears to be no any evidence of attention by the police to the sanctity of journalists' sources, nor for the role of whistle-blowers who are also supposed to be protected by the law.

Inquiries by the Interception of Communications Commissioner and the Home Affairs Select Committee are clearly much-needed and welcome. The public, as well as the media, want to be reassured that the police are only using RIPA in the way Parliament intended, and certainly not to undermine or attack genuine journalistic inquiries into matters of public interest.

Regardless of the outcome of the inquiries the Society of Editors would like to know how the Government intends to ensure that important protections for journalists and whistle-blowers can be reinforced.

I look forward to hearing from you.

Yours Sincerely,

Bob Satchwell
Executive Director

Professor Peter Sommer

Submission to the Joint Committee on the Draft Communications Bill

Summary

This submission concentrates on the technical feasibility and efficacy and value for money of the policies behind the draft Bill. The Bill's aim is to realise the ambitions of the Home Office's Communication Capability Development Programme (CCDP).

The role of retained communications data in investigations needs to be understood within the broader context of all the available potential strands of evidence available for consideration. The ever wider use of computers and telecommunications by individuals, businesses and governments has had a transformative effect on many types of criminal and intelligence investigation. Retained communications data is but one element and while over time some forms are becoming less available, this loss is more than balanced by the increased availability of other types of digital evidence.

The precise problems associated with communications data are best addressed by looking at the various types of Communications Service Provider and the classes of data they might retain. The globalised percentages approach of the Home Office misleads. Many forms of communications data will continue to be available for the foreseeable future without new legislation, while others are held by businesses outside the easy jurisdiction of the UK courts, raising the question of how UK laws, orders, and court decisions can in practice be enforced.

A key requirement of any law is that it is easy to interpret. It is now increasingly difficult to align and interpret the legal definitions of "communications data" and "content" with the complex ways in which data is transmitted over the Internet. Resort must be made to expensive hardware to apply a very large number of technical filters which are supposed to reflect the statutory definitions. These filters must be constantly updated and added to, to reflect the incredible dynamism of the Internet. Even then one can anticipate some of these will require testing in the courts. The complexity and difficulties also have an impact on the extent to which Parliament can be expected to scrutinise the Orders contemplated in Part 1 of the Bill, and to which the regime can be effectively overseen by the Interception of Communications Commissioner.

The penalties for incorrect separation of communications data from content fall chiefly on the police. The regimes for access are very different – interception of content requires a warrant

from the Secretary of State, communications data an authorisation from a senior designated officer. Communications Service Providers are *de facto* protected from mistakes, but police who have acquired material *ultra vires* will find themselves in difficulties, not the least at disclosure and the possibilities of arguments about abuse of process. The problem is significantly compounded by the UK's almost unique position in treating intercepted content as inadmissible and not referable to in legal proceedings.

The Request Filter proposals in cl 14-16 appear to be an attempt to overcome the twin problems of interpretation and the two entirely separate regimes for communications data and the interception of content. But making this a function, direct or delegated, of the same Secretary of State who also issues interception warrants and Orders under the Draft Bill is surely a mistake; if there is to be a credible and viable independent filtering agency much more needs to be said about its resources and governance.

The costs of the Home Office's proposals are impossible to calculate as there are too many unknowns but it is possible to identify criteria for likely value for money. Neither the Explanatory Notes nor the Impact Assessments discuss the source of funding but it seems reasonable to assume that in the current economic climate funding will have to come from existing resources. It is thus useful to seek to evaluate the role of the features of retained communications data that would be enhanced were the Home Office's proposals to be accepted against the loss of some funding to other existing forms of investigative activity and evidence.

Those who seek to avoid having their Internet activities being monitored will have a number of easy routes, even after significant public expenditure on the CCDP. There is a danger that CCDP will have ever-expanding technical ambitions as the Internet changes which, coupled with the need for secrecy, will lead to runaway costs.

I suggest that ways forward include:

- bringing interception evidence back into admissibility so as to simplify many of the technical interpretative problems the draft Bill creates

- continuing the current position that the requirements of domestic CSPs to retain communications data is limited to records they create as part of their regular business activities

- a substantially revised system for the issuing of warrants and authorisations coupled with more robust and credible forms of oversight, so as, among other things, to persuade critical non-UK-based Communications Service Providers to accede to the requests of the UK authorities.

This submission concentrates on the following questions in the Joint Committee's Call for Evidence: 1, 2, 5, 6, 11, 13, 17, 18, 19, 22, 24, 25, 26.

References to comments made in earlier oral evidence sessions are to the uncorrected versions published on the Joint Committee's website.

CV

1. I am currently a Visiting Professor at de Montfort University and a Visiting Reader at the Open University. For 17 years I was first a Visiting Research Fellow and then a Visiting Professor at the London School of Economics. My academic specialisations are cyber security, cybercrime, digital evidence and cyberwarfare.

2. I have acted as an expert witness , for both prosecution and defence, in many trials involving complex computer evidence since 1994. They include: global hacking, terrorism, "phishing", software piracy, murder, large scale illegal immigration, narcotics trafficking, art fraud, state corruption, money laundering and paedophilia. The computer evidence has included the examination of hard disks and other media, the interpretation of network traffic, Internet-related artefacts and communications data. I have also been instructed, in the UK and abroad, in cases involving intercept evidence, including to ETSI standards.

3. My practical work as an expert witness has brought me into frequent and direct contact with many specialist police units. I have provided advice for the UK's National High Tech Crime Training Centre, was the external evaluator and then external examiner for the MSc in Computer Forensics at the Defence Academy which is widely used for police training and while it existed I was the Joint Lead Assessor for the digital element in the Home Office-backed Council for the Registration of Forensic Practitioners.

4. Based both on my academic research and my practical experience, I hope to be able to assist the Committee. I make this submission in a personal capacity. A full CV is available at http://www.pmsommer.com/PMSCV012012_std.pdf

Digital Evidence Landscape

5. The requirement for and cost-justification for an enhanced regime for retained communications data needs to be tested in the context of the vastly increased range and extent of many types of digital evidence available to the UK authorities since the passing of the Regulation of Investigatory Powers Act 2000 (RIPA).

6. Over 75% of the UK population have access to the Internet from their home and each UK household on average owns three Internet-enabled devices[1]. Nearly 80% have at least one home computer[2]. Costs of hard disk storage fall by 50% every 18 months – a 1000GB (1 TB) hard disk now costs about £60 - so that in a typical police search warrant execution on domestic premises they can expect to find several PCs of various vintages, plus external data storage devices such as disks and USB memory sticks. There are 130 mobile phone contracts per 100 of the population, 39% of

[1] Ofcom, Q2012, http://media.ofcom.org.uk/facts/

[2] ONS, Selected Consumer Durables, http://www.ons.gov.uk/ons/rel/family-spending/family-spending/family-spending-2011-edition/sum-consumer-durables-nugget.html

them smartphones, in effect powerful ultra-portable computers[3]. Nearly all of these devices contain substantive files, copies of emails sent and received and histories of such Internet activity as websites visited, pre-occupations of and research carried out by the owner. PCs may also contain artefacts relating to other types of Internet services used, complete with user names and passwords. They may also provide strong evidence of persons with whom the computer owner has been in contact. All mobile phones will contain some records of calls made and received and copies of SMSs made and received – Ofcom says 200 SMSs are sent per person per month[4]. Smartphones will contain much more recoverable data.

7. All of these are key sources of digital evidence and none fall within the regime of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Draft Bill, which are solely concerned with data in the course of transmission. Significant types of evidence that can be obtained under RIPA powers can also be found on seized PCs and mobile phones; and the recovered data will have a considerable historic element because of the capacity of the associated storage devices. Computers and mobile phones are normally seized under powers within Part II of the Police and Criminal Evidence Act, 1984 (PACE) but there are also many additional powers in other legislation[5]. Whereas the RIPA route will exclude "content" for admissibility purposes[6], the same material if found on a hard disk is fully admissible.

8. Over the last 12 years, since RIPA came into force, the amount of information collected by commercial bodies about individuals has increased greatly, chiefly through "get to know your customer's interests better" Customer Relationship Management (CRM) software and the development of commercial credit and marketing databases.[7]Commercial marketing-type data can be bought by law enforcement agencies on commercial terms, privately-held data can be acquired via Production Orders under PACE, subject to the provision of a certificate under s 28 or 29 of the Data Protection Act 1998.[8] The same route can be used to obtain information about banking and credit card transactions – credit and debit card data may also contain information of the location at which a transaction took place.

9. At the same time the availability of Closed Circuit Television (cctv), both officially and privately owned, has expanded greatly, both in the quantity of cameras[9] and their locations and in the quality of images.[10] The UK's National Policing Improvement Agency operates a national DNA database, which is one of the world's largest, with profiles on an estimated 5,570,284 individuals as of 31 March 2012. It also operates a national automated number plate recognition system, which by March 2011 was receiving 15 million sightings daily, with over 11 billion vehicle sightings stored. A

---

[3] Ofcom *Communications Market Report 2012* http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_0.pdf

[4] http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_0.pdf

[5] Eg s 14 Computer Misuse Act 1990 and s 114 Finance Act, 2008

[6] S 17 RIPA 2000

[7] Eg DataHQ, Experian, Equifax. http://www.graydon.co.uk/, http://www.world-check.com/

[8] See also *Government Access to Private-Sector Data*, Brown, International Data Privacy Law, 2012 (in press)

[9] Cheshire Constabulary estimated in 2011 that there are 1.85m CCTV cameras in the UK, 1.7m of which are privately owned

[10] See BBC research in 2009 on the density of local authority-owned cctv cameras: http://news.bbc.co.uk/1/hi/uk/8159141.stm and a Channel 4 News assessment that in 2008 there was a cctv camera for every 14 citizens. http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167.html

national fingerprint database contained 8.3m individual's prints in April 2010.[11] Another new-ish method for tracking the movements, at least of people in London, is via the Oyster card[12].

Types of Communications Service Provider

10. There are several distinct types of organisation and business subsumed under the phrase "Communications Service Provider". By identifying them we can more easily see what potential evidence they might produce, what role that evidence could have in investigations and what obstacles the authorities may encounter. Several important forms of communications data are not under threat of diminution in value as a result of technological developments.

11. Individual businesses may offer combinations of these roles and there may also be a limited amount of blurring of functionality.

12. **Telcos** These are the conventional telephone companies, offering either fixed or mobile services. In terms of communications data, they use and all telcos can provide: the identity of subscriber[13] and for each call: counter-party number, time and duration of call. Mobile phone companies can also provide location data (which is based on the technical requirement for the mobile phone system to know where each of its subscribers' phones is located so that they can be actuated to receive an incoming call). Mobile phone call data records also include the hardware identity of the handset (IMSI) and the SIM in use (IMEI).

13. All telco-related communications data is useful in building up patterns of calls between parties, perhaps to show some form of conspiracy; mobile phone location data additionally shows the movements of a cellphone owner by time over a landscape. Police routinely use special link analysis software to show the patterns of usage[14] and a number of companies also offer Cell Site Analysis to show patterns of movement. Although some fixed line calls may over time migrate to Internet-based telephony (VOIP, Skype), the use of mobile phones is unlikely to diminish and however these phones are used, so long as they are switched on, they will continue to deliver location data.

14. **Network Access Providers** This is what most people regard as Internet Service Providers. The core service is to give the subscriber some form of box (hub) through which the Internet may be accessed. The actual service may be superimposed on a conventional telephone line or entertainment tv cable, or may involve a dedicated line, perhaps fibre. A Network Access Provider (NAP) usually thinks of itself as a conduit. In addition to the basic facility there will usually be others, to handle conventional email, to improve the experience of using the world wide web (for example by

[11] www.npia.police.uk
[12] http://news.bbc.co.uk/1/hi/england/london/4800490.stm
[13] But not for PAYG customers; additional forms of matching are needed to identify them
[14] eg I2; http://www.i2group.com/uk

caching), and the same business may also offer its subscribers hosting facilities, for example to provide a base for a web-server from which the subscriber can publish their own information.

15. NAPs can provide: details about their subscribers[15] and also which of their subscribers held which IP addresses at particular points in time.[16] The latter is especially important as the originating IP address of a communication is routinely gathered in many types of Internet transaction such e-commerce, e-banking, use of file-sharing services, and it then becomes possible to associate the IP address with a subscriber or an individual. The NAP also provides a very convenient collection point at which to monitor the activities of their subscribers, subject to legal constraints. Nearly all large NAPs will have already have installed Lawful Intercept facilities (as required under s 12, RIPA, 2000) and they are also the logical place where any filtering to retain communications data might take place.

16. Under the Bill NAPs will bear the burden of carrying out the filtering functions; in effect their role will change from merely retaining data routinely generated as part of their business functions – for billing and quality of service purposes – into collecting data about their customers for which they have no business use but which may be required by the Secretary of State.

17. **Private Business Networks** As the name implies, these are networks run by businesses and organisations for their own benefit or to serve the requirements of a discrete industrial, professional, academic or other community. They are typically run on equipment owned or rented by the organisation. These days they nearly all use the same technical protocols as the Internet (TCP/IP). General admission to the public is not allowed; many private networks have gateways, some limited, to the public Internet. Private Business Networks still fall within the remit of the Draft Bill - (ss 1(3) and 2(1) RIPA, 2000) and more particularly if the private network is facilitating a communication onto a public telecommunications network.

18. Because they have control over the network, owners and managers have complete technical access to all traversing traffic, though lawful surveillance may be limited.[17] There may also be extensive logging to record accesses by users, visits to websites and the activities of anti-virus software. If a RIPA approach does not prove effective, the same information could be obtained by Production Order or, *in extremis*, by a PACE or similar warrant to seize records and hardware,

19. The authorities might incur difficulties in getting access under RIPA or other means if the private network is managed from overseas and is uncooperative. RIPA covers all situations where the traffic crosses the UK, but enforcement would then require resort to a Mutual Legal Assistance Treaty, the outcome of which could be unsatisfactory.

20. **Social Network Service Providers** This rather awkward phrase (SNSP) encompasses businesses who offer communications and information services via a web-interface or phone/tablet app. The services are sometimes described as nomadic,

[15] The NAP/ISP can only provide information about their subscriber, the person with whom they have the contract, that may only indirectly point to who was actually using the equipment at the time

[16] An explanation of IP address appears from para 37 below. The availability of data is unlikely to be changed as a result of the migration from IPV4 to IPV6.

[17] Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

as they are available whereever there is an Internet connection. Examples include the web-based email facilities of Microsoft (Hotmail, Live, Outlook.com), Gmail, Yahoo and many others. It also includes businesses that offer social networking such as Facebook and LinkedIn and Internet indexing facilities such as Google and Bing. Many Voice-over-Internet-Protocol (VOIP) services, including Skype, fall into the same category.

21. Cloud-services are a variant: they offer remote storage and remote processing; examples are Google Apps/Drive, Microsoft SkyDrive, DropBox, Amazon Elastic Computing, Windows Azure and Apple iCloud. The same provider may offer more than one facility: Microsoft and Google both offer Internet-indexing, web-based email and "chat" (real-time conversation via keyboard); Google provides social networking as well Internet indexing and email, Facebook provides a messaging service, Skype, primarily a VOIP service also offers text messaging and so on.

22. A yet further variant are sites offering participation in online games; in some of them whole virtual worlds are created, participants can create avatars of themselves and chat to other participants; a leading example until recently was Second Life; a number are now delivered via games consoles such as Xbox. Concern is sometimes expressed that these services can be used for covert messaging between criminals and others, though I have been unable to identify any verified instance.

23. The headquarters of the legal entities behind the vast majority of SNSPs are based outside the United Kingdom, which means that non-cooperative enforcement of UK law is difficult. Most are based in the United States. The UK would have to rely on the operation of Mutual Legal Assistance Treaties (MLATs) and these can be slow in process because of the need to follow a variety of local protocols; they also rely on the enthusiasm of law enforcement agencies in the countries in which the SNSP is located. Many larger SNSPs have technical facilities – computer server farms – located in many jurisdictions all over the world, so that identifying where any particular communication or transaction is physically taking place may be almost if not entirely impossible.

24. SNSPs will have limited subscriber data as for many the enrolment process relies on the voluntary supply of information, which is often not verified; most do not impose a charge for their basic services, so that there is no linkage via the banking/credit card system. However IP address data may be collected so that an individual may traced that way (see above). However SNSPs often collect large quantities of *content*; for some the business model consists of giving desirable information or facilities to customers in order to collect information about them which in turn can be translated into opportunities for targeted advertising. In investigatory terms the content may be directly invaluable and may also help identify individuals even where those individuals have sought to obscure who they are. Cloud suppliers also store large quantities of their customers' data files; these presumably could be available to investigators, subject to the appropriate legal processes.

25. Many of these services use *https*, the secure encrypted form of the web, and which is also the foundation of web-based electronic commerce and banking. Encryption is used, not to thwart law enforcement but to protect customers from criminal eavesdropping. But the use of *https* also makes the type of NAP monitoring to obtain enhanced data retention contemplated in the draft Bill much more difficult to achieve.

26. In the US attempts are being made to bring SNSPs into the lawful intercept framework of CALEA (Communications Assistance for Law Enforcement Act, 1994, as amended) which would imply, in the US at least, an interception capability – although this could be provided using software on SNSP servers, rather than the interception of communications "on the wire".

27. The Joint Committee will undoubtedly be making its own enquiries of SNSPs but informal indications are that some US-based SNSPs are willing to respond informally in a positive and timely fashion to UK RIPA-type requests. However in so doing they have to consider, among other things, their obligations under US law, the impact that knowledge of their co-operation has on their customers and hence their business, and concern that authorities in other jurisdictions would want similar facilities. What is likely to be persuasive is the fairness and transparency of the ways in which requests (which would otherwise be warrants and authorisations) are made and by whom, how any material supplied is subsequently handled, and the quality and extent of oversight and audit.

28. **Small-scale informal private network service facilities** This equally awkward phrase covers the situation where communications and information facilities are set up on the Internet by individuals and small groups to service the need of small communities. Although the services are available on the Internet, access is restricted and may be only available by payment or specific invitation. Examples include bulletin board systems (which also have private messaging), private chat systems, file sharing systems, and secure email (which operates outside or in parallel with public email).

29. These services require only modest levels of technical skill to set up. Software to create the basic infrastructure is readily available, much of it at low or no cost. It is easy to run such services with cryptographic protection (*https* and its e-mail equivalent). Many ISPs offer hosting facilities, that is, the use of computers already connected to the Internet and to which the customer can upload his own software. It is also possible covertly to set up such services on large computer systems which are insecurely managed

30. Many of these services are non-sinister; for example bulletin board systems may serve people with particular professional or leisure interests. But the same technical infrastructure can facilitate illegal enterprises.

31. The opportunities for the authorities to detect such sinister services by routine as opposed to targeted Internet surveillance are very limited. The normal methods of detection are via traces left on the computer of one of the participants, confession or infiltration of the membership.

32. **Other forms of covert Internet communications** At this point we also ought to consider other forms of covert communications across the Internet, typically using existing Internet facilities and protocols in ways so that messages and data can be sent without easy detection. It can be a mistake to believe that covert Internet communication is only possible through the deployment of a sophisticated technology. Messages can be published via email, web sites, social networking sites where the words though innocent in appearance, have particular meaning to individuals; it is trivially easy to publish web-pages and files which are not directly

indexed on an otherwise innocent site and which could therefore only be found by those with specific instructions. More sophisticated methods of concealment are also available, but they require greater levels of skill in participants.

33. Almost none of these covert communications will be detected by routine Internet monitoring.

Communications Data and Content

34. Laws, in order to work, need to be capable of easy interpretation. One of the great weaknesses of the draft Bill is that the definitions of communications data do not align with the reality of the circumstances the Bill is supposed to be regulating and managing. At the heart of the Home Office's proposals is a belief that it is possible easily to separate content from communications data.

35. The penalties for incorrect separation of communications data from content fall chiefly on the police and other agencies. The legal regimes for access are very different – interception of content requires a warrant from the Secretary of State, communications data an authorisation from a designated senior officer. Communications Service Providers are *de facto* protected from mistakes[18], but police who have acquired material *ultra vires* will find themselves in difficulties, not the least at disclosure and the possibilities of arguments about abuse of process. [19] The problem is significantly compounded by the UK's almost unique position in treating intercepted content as inadmissible and not referable to in legal proceedings.[20]

Packet communications

36. In conventional analogue telephony, the distinction is easy to make.[21] "Communications data" consists of an enhanced telephone bill (traffic data, who called who, when, and for how long) and information about the subscriber. The content is the voice component, what would be captured if a tape recorder or similar were placed across the line. In mobile telephony, location data is also provided but is clearly separable from the voice element.

[18] They protected *de jure* under s 3(3), RIPA in that they are allowed to view intercept material for the purposes of separating it from content. In the event of inadvertent release they would argue absence of *mens rea* and also invite the CPS to apply a public interest test.

[19] See, for example the Codes of Practice on the *Disclosure and Acquisition of Communications Data* and *Interception of Communications* issued under s 71 RIPA and in particular Chapter 7 of the second Code. See also the *CPS Disclosure Manual* and in particular Chapter 27.

[20] See, among others, *Telephone Tap Evidence and Administrative Detention in the UK*, John R Spencer *in A War on Terror, ed Wade & Maljevic, Springer verlag 2010* and *Intercept Evidence: Lifting the ban,* Justice, 2010, Privy Council Review Chilcot, .Cm 7324,

[21] I am conscious how useful illustrations and demonstrations might be at this point but am also mindful of the restrictions in normal Parliamentary publishing. I would be happy to provide Committee members with a series of demonstrations if they feel it would aid their understanding

37. **Data packets** While in conventional telephony a permanent unique communications link exists between the parties for the duration of the call (a series of switches creating the link for as long as it is needed) , Internet traffic of all kind is transmitted as a series of packets. The system makes much more efficient use of available physical links; each link may convey large numbers of "conversations" or "transmissions". Data to be transmitted is broken down into a series of small chunks ("packets") each of which contains: the address ("IP address"[22]) of the originator, the IP address of the intended recipient, some supervisory information in case packets arrive at their destination out-of-order and need to be re-assembled correctly, and "payload".

38. **Packet payload** may include what RIPA regards as communications data and also what when captured becomes a RIPA interception. But there will also be a series of structures – commands, labels or values – which are the building blocks of the many protocols that make up the Internet – email, web-services, secure web-services, file transfer, file-sharing, Voice-over-Internet. These commands are not normally seen by the regular user; some of these commands and labels may themselves be either RIPA "communications data" or RIPA "content", or may help identify the subsequent sequences of text, etc. as either "communications data" or "content"."

39. **Contents of web pages** The complexity does not end here. A single web page may contain, at least in the terms hoped for in the draft Bill, both "communications data" and "content". A typical example would the "inbox" of a webmail service. The identity of the sender and the time of transmission is "communications data", but the subject matter is "content". On an individual basis visual inspection may easily spot the difference, but what is required is that the separation be carried out automatically at very high speed by software; each individual different design of a webmail web-page would need separate attention and whenever a specific webmail service has a changed design, the technical instructions for scraping the communications data from the content may need to be altered as well.

40. As if this is not enough, modern techniques for creating web-pages rely on taking material from multiple sources and using programming facilities loaded into the web-browser, the page is only finally assembled on the individual user's computer. (This technique relies on variants of JavaScript and HTML). In order to reconstruct from monitored packets the web page that the user sees – and hence be in a position to apply the legal definitions of "communications data" and "content" - several different packet streams may have to be assembled and reviewed. Some of the packets will contain fragments of the Javascript, etc. miniature programs.

41. **DPI** The basic tool for examining packets is called Deep Packet Inspection (DPI); it can operate in software in situations where traffic levels are low, but for high traffic levels (as when monitoring all communications by very many users), specialised hardware must be deployed. All DPI software and hardware arrives with an inbuilt-knowledge of the main Internet protocols of the time and can perform basic analyses on a per-packet basis. But any additional features require the writing of specific

[22] IP addresses are relatively unique to an individual computer; under the present system, IPV4, the ISP/NAP assigns IP addresses to their individual customers and maintains a record of such assignment, usually via the RADIUS log. Large organisations have permanent IP addresses which can be looked up via the Internet "whois" facility.

filters. Where the analysis requires several packets to be considered for their effect together, as in the complex web-page and JavaScript etc. facilities described above, the capabilities of DPI equipment to handle large amounts of data automatically and rapidly are unknown.

42. DPI equipment can usually only work where the web page instructions and components are sent unencrypted. But services from the likes of Google, Facebook, web-based email, are now delivered in encrypted form – using *https* – not deliberately to thwart the police and Agencies, but to protect their users for eavesdropping by criminals. For practical purposes in these circumstances, the only entities that can separate communications data and content are the Googles, Facebooks, and owners of webmail services, which I have referred to as Social Network Service Providers.

43. **Request Filters** As noted above at paragraph 39, an apparent individual communication may involve several different CSPs, a typical example being webmail or social networking. A subscriber's Network Access Provider would only be able to capture the identity of the machine to which the subscriber was connecting – cl 28 (2) and (3). The Social Network Service Provider might recognise that a customer/member was in communication with another customer/member but might lack detailed and authentic knowledge of who that customer/member is. The NAP does know, however, because the subscriber is identified when they pay – by direct debit or standing order – for the network access service.

44. The Bill, cl 14-16 and ENs 73-93, envisages an entity separate from both the CSP(s) and the requesting law enforcement agency which analyses a specific problem, requests material from the respective CSPs which will probably include "content" along with "communications data" and then combines them so that there is a resulting clearer identification of who is communicating. The process, so it is hoped, will prevent the requesting investigating agency from seeing anything other than communications data. In terms of webmail it will enable the requesting agency to see that their person of interest, who is now clearly identified from data supplied by the NAP accessed the webmail service and via it exchanged emails (or other messages) with a number of individuals at particular times. But the requesting investigating agency would at no stage see the subject matter of the messages. This is also the explanation offered by Peter Hill at Q94.

45. Cl 14-16 have a number of safeguards in that necessity and proportionality tests must be applied throughout, there must be rigorous security, after the delivery of the filtered material any remaining material obtained by the Request Filtering Entity in the course of their work must be destroyed, and audit records kept for scrutiny by the Interception of Communications Commissioner. However if these safeguards are not rigorously applied and fully examined by the Interception of Communications Commissioner there is a risk that that what is described as "request filtering" becomes large-scale data mining; the necessity and proportionality tests need to be applied not to just the individual data streams as supplied by CSPs but to the likely effect when they are assembled together.

46. The main purpose of this complex arrangement seems to be to protect CSPs and law enforcement agencies from the situation where the requesting investigating agency inadvertently receives "content" with the consequences indicated at paragraph 35 above.

47. Doubt must also be expressed about the credibility and viability of the entity that performs the Request Filter. Could it really be the same Secretary of State who also issues interception warrants under RIPA Chapter 1 and who also issues the Orders under cl 1 of the Draft Bill? If it is to be a separate "designated public authority" as suggested in cl 20(1) it will need resources, among them highly skilled staff who are familiar with the law, the applicable technologies and police investigative procedure – and who can also act independently. They will almost certainly need high levels of security clearance. In the private sector such people are likely to earn fairly high income; moreover they will want some form of career structure and stability. But there may not be a sufficiently consistent flow of work to make this possible.

Practicalities and Interpretations

48. The process of separating communications data from content is thus theoretically as follows:

    - In the first place the communication must be viewed as the participants would normally see it and the legal definitions in clause 28 (2-5) applied.

    - This must then be converted into instructions which the DPI interception equipment can implement; this in turn implies a full understanding of the various protocols in use for the main Internet services as well as the construction of certain web pages which contain both communications data and content.

49. Some aspects may be easier than others, for example cl 28(2)(b)(iii): "comprises signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of the communication". This sub-clause more-or-less reflects something that can be recognised at a technical level. But others do not.

50. The Bill has a number of clauses in this area that look as though they are capable of several interpretations. For example cl 28(3):

    Data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication is not "traffic data" except to the extent that the file or program is identified by reference to the apparatus in which it is stored.

51. This is borrowed from s 21(6) RIPA, 2000. One particular problem is the status of web pages within a website – the identity of the website is communications data, the web pages within it are content, but what happens if the filename of the web page gives an indication of its content? An example: "http://www.independent.co.uk/news/uk/crime/rebekah-brooks-and-andy-coulson-conspired-to-hack-milly-dowler-and-600-others-7966265.html"

52. Or cl 28(4):

    "Use data" means information—(a) which is about the use made by a person—(i) of a telecommunications service, or (ii) in connection with the provision to or use by any person of a telecommunications service, of any part of a telecommunication system, but (b) which does not (apart from any information falling within paragraph (a) which is traffic data) include any of the contents of a communication."

53. What would be the position of a website which builds up a profile of its customers' activities in order to make them future offers based on previous sales – like Amazon? Or a social networking site that similarly collects information about its user so that *inter alia* it can make recommendations? Both Facebook and LinkedIn frequently suggest "People You May Know" as suitable to add as "friends" – based on previous activity.

54. Simple interpretation of web pages generated by social networking sites such as Facebook may also be surprisingly difficult; here there can be significant problems in identifying which elements on a web page are communications data as opposed to content even before we attempt to turn these into technical instructions. Do we take it that the identities of posters are "communications data" and what they say (or pictures they put up) is "content"? What is the effect if some postings are only available to selected viewers – "Friends" - as opposed to being published to the world at large? What is the position of one-to-many communications but which still fall short of general public publication?

Implications for clause 1 Orders

55. The structure of the Bill is that it is provides a framework, with the detail to be covered by Orders to be issued by the Secretary of State. EN22 sets out the intentions:

> In practice, it is likely that an order under clause 1 may, amongst other things, impose requirements on operators to: generate all necessary communications data for the services or systems they provide; collect necessary communications data, where such data is available but not retained; retain the data safely and securely; process the retained data to facilitate the efficient and effective obtaining of the data by public authorities; undertake testing of their internal systems; and co-operate with the Secretary of State or other specified persons to ensure the availability of communications data.

56. Clause 2 sets out the requirements that Ofcom, the Technical Advisory Board (TAB) set up under s 13 RIPA (and which I understand has until now hardly ever met), and relevant stakeholders must be consulted. But the main democratic safeguard is supposed to be that Orders are subject to affirmative resolution by Parliament - cl 29 (2).

57. Given the pressures on Parliamentary time and material that will be technically complex and outside the normal experience of most Parliamentarians, it seems highly doubtful that detailed consideration will take place. Any such discussion would require information about the precise nature of the threats and, based on what ACC Gary Beautridge said to the Committee in oral evidence (Q 152), the police will want to discourage public debate as they fear that might inform criminals and others of gaps in law enforcement capability. In effect, Parliamentary affirmative resolution will not be a safeguard.

Costs, Value for Money

58. The Impact Assessment accompanying the draft Bill estimates costs to be £1.8bn for the 10 years from 2011/12 without allowing for inflation, VAT and depreciation. The main assumptions are: the total volume of internet traffic increases tenfold over 10 years, CSPs retain data for 12 months, data storage costs decrease by 25% per annum. Of the £1.8bn, £859m is the estimated cost to the private sector – CSPs of all kinds – and which will be paid for by the Home Office. The balance is made up of costs likely to be incurred in management and facilities by law enforcement and the agencies and in oversight by the Interception of Communications and Information Commissioners[23].

59. One of the unfortunate features of the Impact Assessment is that the only bodies listed as formally consulted were the users of communications data, as opposed to the CSPs who are expected to provide it[24]. It is puzzling how costs could be calculated without their input.

60. Forecasting anything to do with the Internet is fraught with uncertainty. Looking back over the last 10 years one must point out that the earliest manifestation of Facebook, one of the key concerns behind this Bill, dates from 2004 and was only opened to the public-at-large in 2006. MySpace, its predecessor in popularity, was founded in 2003 and in June 2006 was more-visited, at least in the US, than Google[25] but it was overtaken by Facebook by April 2008 and by August 2012 had declined to being the 166th "most visited" Internet site[26]. Twitter dates from March 2006, Google Apps, its consumer orientated cloud service of email, online calendar and remotely-stored and editable documents was fully launched in July 2009[27]. Skype, often cited as a particular problem for investigators, was founded in 2003 and has been through a number of versions.

Cost and Benefit Estimates

61. The Home Office Impact Assessment seems solely based on increases in the total volume of Internet traffic, not on its increasing complexity and level of change, which is what any form of separating of communications data from content will have to be concerned with. Even forecasts of traffic volumes over 10 years are problematic; looking simply over the next three years much will depend on the rate of roll-out of high-speed fibre-based links (which by themselves would encourage greater usage) and also to take-up of video-on-demand services, in which customers see films not over the air (terrestrial, satellite, conventional cable) or by renting DVDs, but by receiving video over the Internet.[28]

62. Similar doubts must exist of the estimate of benefits, which are suggested as being between £5 and £6.2bn. The Impact Assessment says:

> These benefits are assessed by operational stakeholders and, using a model validated by HM Treasury, translated into economic values. The assessment takes into account an analysis of criminal behaviours by the Serious and Organised Crime Agency and an analysis of the future communications market

[23] See also Charles Farr's reply at Q73.
[24] Paragraph A3 of the Impact Assessment.
[25] http://news.cnet.com/Googles-antisocial-downside/2100-1038_3-6093532.html
[26] http://www.alexa.com/siteinfo/myspace.com
[27] http://googleblog.blogspot.co.uk/2009/07/google-apps-is-out-of-beta-yes-really.html
[28] See the House of Lords Communications Committee Report: http://www.publications.parliament.uk/pa/ld201213/ldselect/ldcomuni/41/4102.htm

based on OFCOM and other market sources. The largest categories of benefits are direct financial benefits arising mainly from preventing revenue loss through tax fraud and facilitating the seizure of criminal assets. Values for benefits for example from lives saved and children safeguarded are derived from standard estimates by Home Office economists.

63. But if we turn to the main Home Office Research document cited[29] many caveats are made:

> Whilst information on the total and average costs of crime is extremely useful, average cost of crime estimates in this study need to be treated with some caution, for a number of reasons.
>
> _ *Different crimes within the same offence category are likely to have vastly different costs*.
>
> _ *Particular crime reduction initiatives may impact on different types of crime within the same offence category*.
>
> _ *Average cost estimates given…. are best estimates of costs given the information available. However, due to lack of good information in a number of areas, the estimates are inevitably imprecise*.
>
> _ *The costs of an identical crime may fall differentially on different social, economic or geographic groups –*
>
> _ *Some crimes are inevitably costed less accurately than others, and unquantified costs exist which may differ between crimes*. A *comparison* of average costs between different crimes could therefore be misleading. A higher average cost for one crime than for another could reflect the size of quantified, rather than unquantified costs, rather than a real difference in the costs of the crimes to society, although to some extent this is unavoidable in an exercise of this nature.

64. The Impact Assessment's "benefits" have a further problem: they are claims about what would result from the increase in access to communications data over what is currently already available.

65. Whatever the size of the costs and benefits, the Impact Assessment makes a further assertion: "The proposed *10 year* investment in communications data capabilities of £1.8bn compares with an annual cost for policing alone of £14 billion." But this is for every aspect of policing; it may be more realistic to look at the front-line organisations dealing with serious crime. SOCA's resource expenditure in 2011/12 was £427.9m, with a further £34m in capital expenditure[30]. A further basis for comparison is the UK's Cyber Security Strategy from November 2011.[31] The National Cyber Security Programme has a budget of real new money of £650m for the four years 2011-2015, of which only 10%, £65m, will go to the Home Office for "tackling cyber crime". Out of this comes a specific budget for the police: the new National Crime Agency will include the existing Police Central E-Crime Unit, the existing SOCA e-crime and CEOP, the child online protection group. On this basis the estimated costs for the proposed Communication Capability Development Programme begin to look rather large.

Source of Funding for CCDP

66. Even if costs are difficult to calculate it is possible to identify criteria for value for money. One of the great weaknesses of the Bill and the policies behind it is that nowhere has there been any explanation of the source of the required funding. The

[29] http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs/hors217.pdf
[30] http://www.soca.gov.uk/about-soca/library/doc_download/392-soca-annual-report-and-accounts-201112.pdf
[31] http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

government is currently seeking reductions across the whole of public spending costs of 20%, including the police. It seems a reasonable assumption that similar cuts will be expected from the Security and Intelligence Agencies. Only unambiguous evidence of new and growing threats would overcome this. But overall crime is down[32] and the last deaths in the UK from terrorism were in 7 July 2005, although of course this cannot be the sole indicator of level of threat.

67. If we assume that the CCDP will have to be funded from existing resources, the question then arises: which current areas of expenditure will have to be further curtailed beyond the 20% across-the-board savings already demanded? There seem to be two broad choices, either from every form of government expenditure – education, health, defence, transport, social services, etc. – or more specifically from the police and Agencies. One suspects that the police in particular will have reduced enthusiasm for CCDP if they have to partially fund its infrastructure costs.

Essential Criteria for Success

68. If CCDP is to be successful, or value for money, it must have a number of features, not all of which are explicitly referred to either in the Explanatory Notes or the Impact Assessment:

69. DPI equipment must not slow down the Internet experience At present CSPs are simply required to retain business records which fall into the definitions of "communications data". The Bill requires them to process it (see paragraphs 37 ff) and as we have seen these processes can be quite complex; without very high-speed equipment – which implies expense – the user's experience of Internet browsing will be slowed. This outcome would directly conflict with other aspects of Government policy, including that for superfast broadband.[33] DPI equipment installed now would need to be upgraded as fibre-based delivery services are rolled out

70. Monitoring must be near-complete The avowed aim of data retention is that once an individual, hitherto thought innocent, comes under suspicion, investigators are able to discover their past online activities. Although 100% availability of retained communications data seems infeasible, each 1% per cent drop surely significantly weakens the benefits as one must expect that those who wish to conceal their activities will take evasive action. A 90% coverage would incur significant costs but might only capture the activities of the wholly innocent. Thus, every UK ISP, no matter how small, would need to be covered, unless that ISP was only able to function by being a client of a larger, UK-based ISP.

71. The Home Office's position here appears confusing. At Q9 Charles Farr speaks of hoping to get, by deploying CCDP, up to 85% of "coverage" which presumably refers to 85% of communications data being transmitted in and through the UK. Richard Alcock at Q77, says the same but at Q82 says:

> In terms of the general number of CSPs, just in the United Kingdom, I think it is in the order of 250 to 300 communications service providers. We certainly do not envisage working with that many within the piece. Clearly, it depends how communications services change over time and whether groups

[32] http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-march-2012/stb-crime-stats-end-march-2012.html

[33] http://www.culture.gov.uk/publications/7829.aspx

gravitate to a certain service or not. But we certainly do not envisage working with everyone, and I estimate it will be **a relatively small proportion of those**. (emphasis added)

72. This lack of clarity about intended scope of coverage looks odd against the suspiciously precise projected cost of payments to CSPs of £859m.

73. Evasive measures In addition, the proponents of CCDP will need to explain how they would address the obvious easy routes to evading attention:

- Bought-for-cash pay-as-you-go-SIM, giving anonymity
- Use of Internet cafes and other public access services (unless it is assumed that the owners of these services will keep elaborate verified records of the identities of all their customers)
- Hi-jacking of unencrypted domestic Internet access points (with the result that the Internet activity is attributed to the registered subscriber)
- Use of encrypted webmail and other services from providers outside the UK and with whose law enforcement agencies the UK does not have close working relationship
- Use of small NAP/ISPs, thought unlikely to be asked install the DPI monitoring equipment

There are other methods of evasion but the above require no skill on the part of the user, other than to know that the route exists

74. How will encrypted services be handled? As we have seen, an increasing number of large important services are now encrypted, using *https* – see paragraphs 25 and following above. There does not appear to be a *routine* means of decrypting and hence getting access to anything that might be communications data. *HTTPS* is fundamental to Internet-based e-commerce and e-banking. In the course of a targeted investigation it may well be possible to obtain the co-operation of the encrypted service as there will then be evidence upon which judgements of necessity and proportionality can be made[34]. But CCDP is about the routine retention/collection of data from the whole population and in the absence of specific suspicions.

75. A possible solution would be for the CSP to retain all data that appeared to be encrypted and to make no attempt at separating communications data and content until there was a specific request. However, given the quantities of encrypted transmissions, CSP storage costs would soar. But Richard Alcock, Q47, seems to say that RIPA would not allow this, presumably as content, even if encrypted, cannot be retained.[35] And most versions of https can only be intercepted at the time encrypted messages are sent, using a "man-in-the-middle" attack.

76. **How will overseas CSPs be dealt with?** The UK appears to have two routes to dealing with CSPs outside the jurisdiction. The first is to seek their co-operation, a

[34] There are also other technical routes which are available in a targeted investigation in the event of non-cooperation from the service provider

[35] It is possible that the uncorrected transcription on which I am relying is not wholly accurate at this point.

view reflected in Charles Farr's response at Q52: "The central plank of this programme is a collaborative relationship with service providers in this country and overseas. DPI, black boxes, or whatever other metaphor or language we choose, only come into play in certain circumstances when an overseas provider or the state from which an overseas provider comes, or both together, tell us that they are not prepared to provide data regarding a service which is being offered in this country and which we knew and know is being used by criminal elements of whatever kind." This incurs relatively low financial costs but may involve persuading the CSPs that the legal and regulatory framework for issuing requests is fair and rigorous. See my remarks at paragraph 27 above and 92 below.

77. The second route appears in the same answer: "The legislation therefore creates the option, in those circumstances, of putting a black box, using your language, on a UK network across which the data from the overseas provider must move, with the purpose of sucking off that data, under our guidance—"control" is too strong a word—and storing it through that network provider." In other words a form of filtering based on that service. At Q54: he says: "The network provider would take off the network the data particular to the service of concern to us and store all that data. We would then apply to the network provider for specific bits of the data that has been so stored, in accordance with usual practice." This would incur expense and the Joint Committee should make further enquiries as to its likely level.

78. Many of the big overseas services with which we assume there is the greatest concern, like Google, Live/Hotmail, Twitter, Facebook, etc. use encrypted links, in which case this second route would have very limited effect.

Benefit Elements

79. The Home Office express the benefits in terms of globalised percentages, saying that they hope to move from a 75% availability to 85% (Q9). At Q22, Charles Farr produces a percentage breakdown of applications for communications data, presumably based on existing law.

> 27% of data for which applications are made and obtained is for drugs-related offences, 15% is for property offences, arson, armed robbery, theft, 12% is for financial offences, 10% is for sexual offences, 6% is for homicide, 5% is for missing persons, 5% is for harassment, 4% is for offences against the persons, and 4% to 5% is for explosives.

80. But what is really required, if there is to be a proper value for money assessment, is the ability to identify particular types of communications data originating from particular classes of communications service provider. Many existing highly useful forms of communications will continue to be available for the reasonably foreseeable future – including mobile phone location (which is not Internet dependent) and, from Network Access Providers, the ability to link IP addresses obtained by a variety of means to the identities of their subscribers. What is needed is a way of identifying the specific forms of further communications data that CCDP will deliver – so that it can be related to the costs of acquiring it.

81. One purpose of setting out the various types of CSP and the classes of data they might produce in paragraphs 10 to 31 above was to assist the Joint Committee in gaining a

better ability to assess these separate elements. I note the remarks of ACC Gary Beautridge to the Committee in oral evidence (Q 152) and have some sympathy with his concern not to expose current law enforcement weaknesses. But I hope the Joint Committee will pursue with vigour and carefully test any confidential information supplied to it by ACPO and others.

Cost Elements

82. DPI Boxes The first cost element, to be paid for by the Home Office, is the installation of the DPI boxes at NAP/ISPs. Because one must anticipate attempts at evasion by those of greatest interest to the authorities, this investment will have to be front-loaded. That is to say, near 100% coverage of UK NAP/ISPs will be required not too long after the intended start-up. Although the Home Office speak of wishing to run pilot studies, usually an important means of testing a policy, the pilots could not show how well CCDP was meeting the threats of evasion. This significantly increases the risk to the taxpayer.

83. As noted above, given the growth speed, and difficult-to-predict nature of the Internet DPI boxes would need constantly to be upgraded

84. Filtering Software As explained at paragraphs 37 to 40 above, the provision of filters to be run on the DPI hardware is likely to be an extensive and on-going project. It is not clear who will do the necessary research and produce final products – GCHQ might be a candidate. This will still be a cost which has to be met from some budget or other ultimately funded by the tax payer.

85. CSP additional costs In addition to the costs identified in the ENs and Impact Assessment, the Joint Committee should ask CSPs about the costs of producing material from their archives of retained data at speed to meet likely emergency requirements from law enforcement. It is not enough that required communications data is simply kept, it must also be available; and that implies some near online capability. Mobile phone companies, on whom there are frequent demands but where the normal requests are very standardised – calling number, receiving number, date/time, call duration, IMEI, IMSI, location – have automated or semi-automated systems. Will something similar be required of other types of CSP, and what will be the cost implications?

Open-ended nature of CCDP

86. The following elements are highly difficult to forecast: the growth in Internet traffic volumes, the levels of complexity of future Internet services, the numbers of CSPs, and the extent of attempts at evasion. If allowed to proceed in in anything like its current form CCDP will have all the pre-conditions for an uncontrolled government computing project or MoD defence contract. Its details will be shrouded in secrecy in order not to give criminals and others an advantage, any associated contracts will be hidden from scrutiny as "commercially confidential" and the precise specification will be subject to constant change. This is the classic formula for runaway costs and hence a significant risk to the taxpayer.

Possible Alternative Legislative and Policy Routes

87. I hope it will help if I sketch out some alternatives to the proposals in the draft Bill.

88. **Intrusive Data Monitoring Warrant** A more radical form of legislation would almost certainly have *to abandon the attempt to separate communications data from content*, so that an intrusive data monitoring warrant would cover both. This would mean that the peculiar UK position of making intercept evidence inadmissible[36] would also have to be abandoned. RIPA already features directed and intrusive surveillance regimes – s28 and s 32 respectively. The test for granting would depend on the levels of intrusion rather than a technical assessment of whether data was "communications data" rather than "content".

89. Any new power along these lines would almost certainly have to be subject to judicial scrutiny as opposed to the current position where warrants are issued, for historic reasons, by a Secretary of State acting on behalf the Crown. I am aware the arguments for and against of warrants issued by a Secretary of State and of the similar arguments about self-authorisation by designated senior officer in relation to communications data.

90. **Data Retention of Business Records** This would be very similar to the current position where CSPs retain records that they create in the normal course of their business and which would include "communications data" as currently defined in RIPA or EUDRD but would not require them to do any further processing.

91. I would favour passing power this over to judicial scrutiny as well, not the least for the reasons now explored below.

92. **Position of Overseas CSPs, including SNSPs** As we have seen, much of the material which the authorities hope CCDP would make more available is held by CSPs based outside the UK. It seems much more sensible to seek their co-operation rather than relying either on Mutual Legal Assistance Treaties, which can be cumbersome and too slow to be effective, or to hope that the data can be monitored while in transit in the UK. But to do this may require convincing SNSPs that UK legal procedures are fair and transparent. As noted above, SNSPs will need to consider their position under the laws of their home jurisdiction, usually the United States, and also the perceptions of their world-wide customer base.

93. Judicial supervision is far more common and understood worldwide than then UK practices of a politician to grant warrants for the most intrusive activities and self-authorisation by senior law enforcement officer for the rest. For that reason alone, judicial supervision is likely to be more credible and persuasive.

94. There is a further element: companies like Google, Facebook hold large amounts of personal data about their customers and do so with their consent. Cloud providers hold files created by their customers. In these circumstances the assessment of proportionality becomes especially important. Should a warrant automatically give

[36] S 17 RIPA

access to *all* the material the cloud provider holds? To my knowledge this issue has not be examined in any detail anywhere in the world.

95. **Enhanced role of Commissioners** Also as part of a policy of convincing SNSPs and others of the rigour and fairness of UK procedures, there surely needs to be a more visibly robust regime of Interception of Communications and Information Commissioners. Information Commissioners have always had a public profile, appearing on television, engaging in debate and making public demands for law changes and increased resources. Interception Commissioners have until recently been almost invisible. The most recent report[37], for 2011 provides more detail and candour than hitherto, but the Commissioner held just one meeting outside a wholly official environment, with the specialist Data Protection Forum.

96. Although his Report describes how he audits the activities of the police, Agencies and other bodies, it is unclear how far he questions the reasoning and evidence of the "necessity and proportionality" tests that are the starting point for each warrant/authorisation. If he doesn't he should do so – and identify situations where matters went awry. Obviously any review of such tests would have to be on the basis of information available at the time. The Commissioner could also usefully describe in more detail the resources and skills of his inspectors. Consideration should be given to moving this role into the Information Commissioner's Office, where it might be less easily perceived as "captured" by the law enforcement and intelligence agencies it is supposed to be overseeing.

97. The Investigatory Powers Tribunal is even less visible, and hence less credible, than the Interception of Communications Commissioner. It would have much greater perceived independence and credibility if reconstituted directly under the control of the Supreme Court (as is the US Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Appeal), with more transparency.

98. **A new type of retention warrant?** One can also envisage a new type of warrant, also issued by a judge, on the basis that although an individual who is not currently presenting sufficient of a threat to justify full scale monitoring there was the possibility by virtue of people whom they knew or views they were thought to hold, it might be useful if the ISP were to **retain** their communications and content for a period of year against the future possibility that the police or other investigators produced a full warrant to view the material. This would address a problem identified by investigators that on occasion they identify a substantial conspiracy in an advanced stage and wish to know something of the previous actions and thoughts and associates of

[37] http://www.intelligencecommissioners.com/docs/0496.pdf

those thought to be involved. However this last proposal has many difficulties associated with it – what would be the actual criteria for the issuing of such a warrant and how would it be supervised? But it would have the further advantage of being targeted – effort and expenditure would be directed against those who might in the future be of interest, as opposed to the 99.5% of the population who never will be.

I would be happy to answer any questions the Joint Committee may have.

August 2012

Professor Peter Sommer

Submission to ISC Privacy and Security Inquiry

Summary
Both "Privacy" and "Security" are highly abstract value-laden terms - I suggest an emphasis on extent, authorisation for, subsequent management of, and the provision of full audit trails of, means of intrusion which in turn should be related to the harm to be ameliorated. This approach should also be reflected in radical rather than piecemeal reform of existing laws.

1. This is a personal submission.

2. I am currently a Visiting Professor at the CyberSecurity Centre at de Montfort University and a Visiting Reader at the Open University. For 17 years I was first a Visiting Research Fellow and then a Visiting Professor at the London School of Economics specialising in Information System Security. At the OU I am the Course Consultant for a Masters' course module on Computer Investigations and Forensics. I validated the UK's first computer forensics Master's course at the Defence Academy (Cranfield University). I am currently teaching a digital forensics course at the Cybersecurity Centre for Doctoral Training at Oxford University. During its existence I was the Joint Lead Assessor for the digital specialism at the Council for the Registration of Forensic Practitioners, In 2008 I was appointed to the Digital Forensics Specialist Group which advises the Forensic Science Regulator.

3. Most of my current income comes from instructions as an expert witness in complex digital evidence , for prosecution and defence in criminal matters, for claimants and defendants as well as single jointly in civil matters and for international criminal courts. My instructions have involved intercept, communications data and IP address evidence and have included terrorism, global hacking, paedophilia, narcotics trafficking, firearms offences, state corruption, murder, financial fraud, art fraud and money laundering.

4. Between 2003 and 2009 I was a member of the Scientific Advisory Panel on Emergency Response (SAPER) run by the Government's Chief Scientific Advisor, the remit of which included counter-terrorism and involved interaction with JTAC and others. Since the withdrawal of the Draft Communications Data Bill in 2013 I have been providing at their request advice to Home Office officials.

5. The website www.pmsommer.com contains a full CV and pointers to relevant publications, submissions to Parliamentary Committees and legal instructions.

6. **What balance should be struck between the individual right to privacy and the collective right to security?** The issue is easier to resolve if recast in terms of types of intrusion, their justification in specific circumstances as a means of limiting harm, the arrangements by which the need for the intrusion is tested and authorised, how the intrusion is subsequently managed (including for collateral intrusion), and the extent to which each stage is auditable so that, after the event if not during, compliance failures can be detected and remedies made available. The difficulty with the ISC's consultation question, as framed, is that one may end up with little more than a very commonplace and abstract generalisation.

7. It is not enough, either, simply to look at broad classes of technologies; one must consider the many ways in which they can be deployed. As technologies of collection and analysis develop over time, issues of extent of intrusion change as well. It is possible to illustrate this by reference to the two technologies identified by the ISC:

8. **CCTV.** There are many different types and forms of deployment, for example:

Privately owned, Home Office Code of Practice - compliant[i]	Captures all passers-by. Only looks at public locations. Controlled by owner, released to Law Enforcement (LE) and Agencies on request or via Production Order. Has to be manually reviewed. Mostly used after the event, to identify perpetrators and their movements
Local Authority – crime prevention	Captures all passers-by. Only looks at public locations. Controlled by owner, released to LE and Agencies on request or via Production Order. Often viewed live. Has to be manually reviewed. Can detect events in commission but can also be used post-event.
Installed covertly as intrusive surveillance	Installed for specific need under RIPA s 32 – intrusive surveillance (and other Acts). If installed within property – under Police Act 1997 Part III (Authorised by SoS or Senior Authorising Officer) and s 5 ISA, 1994[ii]. Can detect events in commission but can also be used post-event.
Road Traffic + Automatic Number Plate Recognition	Captures all passers-by; 26m+ records per day[iii]. ANPR is captured digitally without manual intervention and stored for many years – provides detail on movements of vehicle and by inference, owners. Can be combined with other data in digital form

Future – facial recognition	Requires combination of high resolution cameras, ability to capture sequence of shots and ability to convert to 3D "face" plus database of suspects

9. **Communications data.** This term, from RIPA, 2000, also covers a number of different circumstances:

Fixed land-line calls – criminal investigation	Call Data Record – who called whom, when and for how long - acquired for all customers and stored by CSP[iv] for 12 months[v]; obtained by LE under RIPA s 22 – requires LE SDO to make judgement about necessity and proportionality
Mobile phones – criminal investigation	Call Data Record as above but also includes geolocation data. Geolocation data , acquired for all subscribers and stored by CSP for 12 months, for all times phone is powered up, not just when a call is being made - shows an individual's detailed movements for all this period. Cell Tower Dump – all phones powered up in a specific area – obtained by PACE Production Order
Web-browsing – criminal investigation	Top level – all website accesses by all subscribers but only up to first back-slash - acquired and stored by CSP for 12 months and obtained under RIPA (this is one area which the Communications Data Bill wanted to alter)
Email activity - criminal investigation	For all subscribers: who writes to whom but not content – 12 month storage by CSP, released under RIPA/Data Retention Directive
Intelligence Agency use of the above	Available under ISA, RIPA and s 94 Telecommunications Act, 1984 but also according to Snowden, by other means as well - acquired and stored by GCHQ – only controls are purely internal - Commissioner reliant on accuracy and completeness of GCHQ records

10. **Testing Intrusion Methods.** It is possible and more useful to identify a series of tests based on principles rather than the existing legislation. The starting point is that the intrusion needs to be justified. Notions of individual

privacy including "correspondence" (which includes phone calls and emails) are deeply embedded in Western and international thinking – Art 12, UN Universal Declaration of Human Rights, 1948, Art 8, European Convention on Human Rights, 1950, and 4th Amendment to the US Constitution, 1789.

11. Looking first at ***effectiveness***: How far and in what ways does the specific intrusion method address the claimed harm?

    - Does the method help directly ***detect*** the harm in the first instance?
    - Is it a potential ***witness*** to harm that has not hitherto been detected?
    - Does it have a supporting role in ***post-incident investigation***?
    - Are statistics and supporting information available to support any claims around the above?[vi]
    - How does it mesh in with other methods of intelligence gathering, such as: open source, self-publicity by would-be perpetrators, alerts from the public and others, information gathered in the course of other investigations, suspicious activity such as the purchase of materiel and training, conventional physical surveillance, CHIS and information from financial institutions?

12. Looking specifically at the ***technological method***:

    - Does the method collect data globally from an entire population or only a small sub-section of which is likely to fall under suspicion?
    - Does the method inevitably collect more data / information from a suspect than is required for the investigation into the alleged harm?
    - What controls exist to limit access to / use of data which is not required or no longer required for the investigations?
    - How easy is it to combine the acquired data with other streams of data acquired by other methods so that the amalgamated intrusion is greater than the sum of its constituent parts?
    - What is the process by which authorisation to acquire / have access to takes place?
    - Where there is routine global non-targeted acquisition of data, is there a separation between the entity that collects that data and the agency that wishes to make use of it – such that on each occasion the requesting agency must justify their requests in terms of necessity and proportionality?
    - Does the intrusion mechanism and any associated controls have implications for trust in institutions in which society has a significant interest, such as the privacy of communications, the central operation of the Internet, and the use of encryption techniques for authentication of parties to a transaction and safeguarding citizens against eavesdropping for criminal purposes? These issues can have, among other things, profound economic implications[vii]. Is there a mechanism, in government and in the oversight apparatus, to ask these questions?

- What policies and procedures exist to destroy data when there is no longer any justification for holding it?
- What audit schemes exist to detect / log usage *ultra vires*?
- What audit / oversight mechanisms exist to verify compliance?

13. Some, but not all, of these questions appear in the current Code of Practice for Covert Surveillance and Property Interference. [viii]
14. **Transforming and Combining Effects of Newer Technologies.** Changes which may appear, moment by moment, to be incremental, can nevertheless have a transforming effect. In relation to intelligence analysis: much more information is generated in digital form as a result of the use of computers, mobile phones and others; costs of collection fall all the time, costs of data storage fall all the time, costs of computer-aided analysis fall all the time. Costs of digital surveillance, compared with more conventional means, fall all the time. Once intelligence material is in computer-readable form it can be readily combined and aggregated[ix] so that while surveillance becomes "easier and cheaper", levels of effective intrusion increase as well. Geolocation data from mobile phones combined with ANPR from CCTV combined with email communications data (which excludes content but identifies to whom an email was sent) combined with web-browsing activity (the web-site but not the individual page) enables the easy drawing of inferences and levels of intrusion which may not have been envisaged when the authorisations for each separate source were given. The data sources can also be readily combined with air passenger movement data, credit-scoring data and financial transaction records.
15. The now-abandoned Draft Communications Bill made an initial (and rather unclear) attempt at managing combined sources of potential evidence in the "Request Filter"[x]
16. There is an argument which is sometimes advanced by the Agencies that, while they may hold quantities of data there is no intrusion unless it is accessed[xi]. The difficulty with this is that whereas in the purely criminal procedure communications data is held by the CSPs and only released to law enforcement after a proper, recorded procedure (s 22 RIPA), in the case of GCHQ, the process appears to be entirely internal. The Commissioners and the ISC are wholly dependent on there being a very reliable audit trail – and their ability to have sufficient technical knowledge to spot where there may be gaps.
17. The argument "we need the haystack to find the needle" [xii] should be tested for actual examples. It also assumes that the Agencies know what a specific "needle" looks like. The greater the volume of data collected the greater the problems of false positives and negatives; the former can lead to false allegations.
18. A further argument sometimes made by the Agencies is that there is no recorded evidence of abuse by them of communications data. This surely cannot be taken as definitive evidence that there has been no abuse. It is helpful to compare not dissimilar institutions, the police and the military, who have to make very difficult decisions rapidly and on imperfect

information. Although these institutions, like the Agencies, are basically ethical nevertheless significant cover-ups occur, for example, Hillsborough in the case of the police, Iraq breaches in the case of the military. Reasons include: to save careers and the desire to maintain "public trust" in the institution. In the case of the Agencies there would also be a perceived need to protect sources and methods. It is part of the stock-in-trade of the Agencies to conceal. It is also worth noting that more than 1,100 DWP staff have been warned over prying on benefits records[xiii] In addition, instances of mistakes by the Agencies in assessment abound[xiv].

19. The scenarios for longer-term concern, even if they could seem remote at the moment, but which any legal and oversight mechanism should anticipate are:
    - Arrogant rogue Agency employees who think they know better than the public and elected politicians[xv]
    - Politicians in difficulty and unable to distinguish party interests from national security and seeking to use information to discredit opponents and limit legitimate dissent

20. Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted. Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

21. It is difficult to provide detailed commentary and proposals within the ISC's requested 3000-word limit. I note the length of the submissions to the courts in respect of the actions by Big Brother Watch, English Pen and the Open Rights Group and Privacy International. I am happy to provide more detail on another occasion.

22. Law reform is pointless unless one also considers means of enforcement. In most instances that implies the availability of admissible evidence. That, and the problems of open courts would create huge difficulties for the Agencies as it would reveal methods. Thus, a reformed law could only be part of a solution to re-assuring the public about Agency behaviour; it would also need to include credible, independent, trustworthy and powerful oversight.

23. There also seems relatively little point at looking at one set of methods of investigation / intrusion without considering the others, in particular those where technological change has transformed capabilities. The other important technologies are:

    - The use of audio and video bugs, the use of hardware to bug or otherwise compromise computers, phones and other devices. These come into the category of "interference with property". For regular policing activities these are addressed in Part III of the Police Act 1997 and for the Agencies under ISA 1994 ss 5-7. Access to a

computer by an "enforcement officer" which would otherwise be an unauthorised access for the purposes of s 1 Computer Misuse Act, 1990, (CMA) is protected under s 10 of the same Act.

- Computer intrusion using software – see also below on illegality.

24. Current surveillance legislation is spread over several laws and subject to a variety of authorisation regimes. RIPA covers intercept (authorised by Secretary of State), communications data (authorised by Senior Designated Officer - SDO), interference with property (bugs, taps) is authorised by Secretary of State (Agencies) and SDO (criminal – under Police Act 1997), CMA s10 allows LE access to computers in the course of their duty but does not cover if such access involves a s3 CMA offence, by using software backdoors – and ISA s 5(1) does not appear to give this power to the Agencies either. Physical seizure of computers under PACE requires a judicial warrant.

25. This confusion is difficult for law enforcement and only slightly less so for the Agencies[xvi]. It is also difficult for politicians and other policy-makers to understand the range of powers. There thus seems a strong argument for a radical revision, similar to that involved in the Police and Criminal Evidence Act, introduced in the 1980s after dissatisfaction with the use of police powers under the old Judges' Rules.

26. My outline suggestions for law reform are thus:

- Research and produce a new integrated surveillance powers law with the emphasis on levels of intrusion, similar to the existing "Directed" and "Intrusive" models in ss 28 and 32, RIPA rather than based on specific technologies. Use Codes of Practice issued under SIs for the detail. The new law should cover intercept, communications data, bugs, taps and computer intrusions.

- Recognise that, because it is now all "data", the distinctions between intercept and communications data are difficult to realise in practice (try applying them to a Facebook page or mobile phone app) so that the issue here too is level of intrusion. Remove the existing inadmissibility rule on intercept[xvii].

- Recognise also that distinctions between "external" communications and those between UK citizens will in practice be difficult to make given the international nature of Internet services[xviii]

- Consider, as an alternative to whole-population data retention, targeted Data Preservation Orders requiring CSPs to collect and hold data (intercept and comms) of identified persons against the time at which a full warrant is authorised.

- While maintaining the role of Secretary of State for authorising Agency strategy and broad operations, place the granting of

individual warrants with judges[xix]. This would be more in line with international practice, provide a "separation of powers" and enable judges to build expertise in surveillance technologies in a way no Minister would ever have time. The argument about Ministerial democratic accountability to Parliament collapses when one accepts they will never discuss operations and methods in public and can thus never be challenged[xx].

- Limit Law Enforcement and Agency powers of self-authorisation to the very lowest levels of intrusion.
- Build into legislation, including ISA, and related Codes of Practice, the need for the maintenance of full audit records
- Add to the oversight remit a specific requirement to consider the impact of Agency activity on society as a whole[xxi]
- Develop a robust route for Agency whistle-blowers

27. Oversight Mechanisms The ISC's Call does not refer to the effectiveness of oversight but, given the problems of testing surveillance law compliance in open court, trust in the quality and depth of oversight becomes crucial. I note that the ISC has yet to publish its Memorandum of Understanding[xxii]. Both the Commissioners and the ISC must acquire resources enabling them to identify and pose questions covering technical surveillance capabilities and how they are deployed.

I would be happy to enlarge on any of these matters.

February 2014

---

[i] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

[ii] Also see Code of Practice: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf

[iii] http://www.acpo.police.uk/documents/crime/2010/201010CRIANP01.pdf; http://www.theguardian.com/uk-news/2014/jan/23/cctv-cameras-uk-roads-numberplate-recognition

[iv] CSP: Communications Service Provider – incorporates Telephone companies, mobile phone companies and Internet Service Providers

[v] Data Retention (EC Directive) Regulations 2009; http://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents

[vi] See http://www.washingtontimes.com/news/2013/oct/2/nsa-chief-figures-foiled-terror-plots-misleading/?page=all#pagebreak; http://politicalscience.osu.edu/faculty/jmueller/NSAshane3.pdf, http://newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1.pdf

[vii] http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10431825/Inventor-of-world-wide-web-criticises-NSA-over-privacy-breaches.html, http://www.bbc.co.uk/news/technology-25033577, http://www.scmagazineuk.com/nsa-backlash-continues-uk-firms-move-data-out-the-us/article/329224/?DCMP=EMC-SCUK_Newswire

[viii] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97960/code-of-practice-covert.pdf

[ix] According to Snowden, the main NSA resource is XKeyscore (http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data) but commercial programs used by law enforcement also provide similar facilities, if on a smaller scale, eg Nuix

(http://www.nuix.com/Investigation) and I2 Analysts' Notebook (http://www-03.ibm.com/software/products/en/analysts-notebook/)

[x]Clauses 14-16, Draft Communications Data Bill, http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf

[xi]David Omand: http://www.theguardian.com/commentisfree/2013/jun/11/make-surveillance-ethical-and-effective

[xii] Iain Lobban in oral ISC evidence, 07/11/2013

[xiii]http://www.telegraph.co.uk/news/10561388/More-than-1100-DWP-staff-warned-over-prying-on-benefits-records.html

[xiv]See, for example, *UK Eyes Alpha*, Mark Urban, *Empire of Secrets*, Calder Walton, *GCHQ*, Richard J Aldrich. Perhaps one can add the examples of Adebowlae and Adebowale, known to the authorities but not tracked. See http://www.independent.co.uk/news/uk/crime/theresa-may-keen-to-revive-snoopers-charter-in-wake-of-woolwich-attack-8629990.html

[xv] *UK Eyes Alpha*, ibid

[xvi] See for example Jemima Stratford QC opinion: http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf

[xvii] S 17 RIPA

[xviii]RIPA s16(2)

[xix] There would be a graduated scheme depending on levels of intrusion

[xx] See Hansard 21/01/2014 col 151, Hague on Dishfire

[xxi] In ISA s10 and J&SA 2013, Part 1 s 2

[xxii] S 2(5-6) J&SA

Talk Talk Group

Talk Talk is pleased to set out below its responses to the questions in the David Anderson QC review of communications data and interception powers.

We would be happy to provide any further information as required in relation to any of our responses. ***

1. What are the changes and developments in communications technology, services or methods that need to be taken into account is by the government in framing legislation on interference[1] with communications? It would be helpful if you could describe the present situation, any changes that have occurred since the publication by the government of communications data draft legislation in 2012, and what you foresee happening over the next five years and beyond.

It is generally very difficult to try and predict specific changes and developments in this area but we would highlight the following likely future trends:

(i) Overall, the direction of travel is that communications increasingly are made over data networks rather than conventional voice networks. This will provide opportunities for 'over the top' (OTT) providers to provide communications services without making large investments in infrastructure (or indeed owning infrastructure) themselves. By way of illustration, we are already seeing evidence of content providers contacting network operators directly to host on-net content delivery services to provide their OTT content. Also many OTTs are based in other countries rather than just the UK.

(ii) ***

(iii) ***

(iv) Furthermore, we expect to see an increase in different access technologies. Fibre networks that are independent of BT are being built across the UK and it is well-known that mobile services and networks are increasing in importance. Allied to these developments is more convergence between fixed and mobile services which means that the customer will be able to use different access methods during a single communications session or transaction.

(v) Finally, it is worth noting the increasing trend of encryption using protocols and services such as SSL and TOR. This trend is driven by network and OTT providers wanting to secure data but also end-users seeking effective tools to address their own privacy concerns.

1 Article 8 of the European Convention on Human Rights sets out that, in accordance with the law, there can be interference by the state with private communications for a range of purposes, such as in the interests of national security and the prevention of crime.

2. Considering the state of communications technology now and anticipated, does the distinction in existing law and proposed in the draft bill in 2012 between communications data and content continue to be valid? How does this distinction relate to relative intrusion into an individual's privacy?

From a technical perspective, metadata of a communication event has been the source of communications data to date e.g. call data records (CDRs) generated for telephone calls. The production of such metadata records has been inherent in the provision of communication capability, often driven by the need to be able to invoice customers for individual events, e.g. phone calls. Looking ahead, a move away from more traditional communication technology may result in a reduction in these metadata records and, as a result, in a blurring of the distinction between communications data and content. ***

Notwithstanding technical developments, we believe that the distinction between communications data and content is clear in the private individual's mind in the sense that they do not expect data retention to extend to "stuff that they write, send or post" to other people. The law must therefore find a way to make this (perceived) distinction in a way that is meaningful in the private individual's mind.

3. Is the subdivision of communications data into subscriber, use and traffic data appropriate for the future; and are the current definitions of those subdivisions right? How does this distinction relate to relative intrusion into an individual's privacy?

There is likely to be a continued need to distinguish between information about the individual who initiates a communication (subscriber data) and information about how and when that communication takes place. The concept of subscriber data was borne out of the commercial need of having someone to invoice for a transaction, e.g. billing a customer for making a phone call. If that need no longer exists, however, the term "subscriber" may no longer suitable but we believe there may still a need to have discrete information that enables identification of the person who initiates a communication. Being able to identify this discrete piece of data would serve to safeguard the privacy of the individual in that other data (e.g. use data) could be deliberately protected from access.

It should be noted however that commercial models are always changing in this fast-moving sector. ***

4. How should the government address the challenges to lawful interference with communication that arise from communications services being provided to people in the UK from foreign countries?

We believe it is essential that communications providers based in the UK, such as TalkTalk, are able to fall back on specific and clear obligations laid down in UK law in order to be able to release any data to relevant law enforcement authorities. There is a concern here that the public perception of UK communications providers has been dented or even damaged because of the recent debate in other jurisdictions over communications providers releasing data to law enforcement agencies under what appears to have been purely voluntary arrangements.

The growth of cloud-based computing, global service providers and technology globalization will mean the provision of service to the UK from foreign countries is likely to be a trend that continues and increases.

***

5. How might communications service providers based in the UK be able to assist in lawful interference with communications should overseas-based providers of communications services not cooperate with the British government?

Our main concern in this regard is that communications providers based in the UK, such as TalkTalk, must be able to fall back on specific and clear obligations laid down in UK law in order to be able to release any such data to relevant law enforcement authorities. *** This will also ensure that the integrity and reputation of communications providers is not adversely affected.

6. Should the government seek a single international regime for the operation of lawful interference with communications? If so, what might be its principal features?

We would be concerned about the potential implications of an international regime for communications providers. By way of example, it would increase complexity and cost of compliance for communications providers if this meant having to comply with requests for data and interception from foreign bodies and authorities.

7. The proposals put forward in 2012 to enable access to communications data depended on certain procedural and technological components, notably the extension of the "single point of contact" and the introduction of the request filter and deep packet inspection. What arrangements would you prefer to see to enable those with lawful authority to obtain communications data or intercept from you and other providers?

The concept of a "single point of contact" within individual law enforcement agencies has worked well and should be encouraged. The framework and controls in place, as provided by RIPA, provide an appropriate level of control over access to communications data.

In our recent experience, discussions with SPOCs are becoming more technical and so communication providers need to consider the technical abilities of disclosure teams in order to answer fully any questions from SPOCs. ***

With regard to the use of request filters, whilst they may make the data request process more streamlined, there is a concern that the use of the same filter across multiple provider data sources may result in information that is not fully comparable. ***

8. How should the government work with communications service providers to address the impact of the use of encryption on lawful interference with communications, particularly if such use is set to increase?

Within the existing legal framework, TalkTalk would be happy to engage in a dialogue with government regarding this growing trend. The rise in the use of encryption should for the most part be positive in securing customers use of the internet. ***

9. What more could be done to exploit the communications data and intercept that is currently available and likely to continue to be so?

We believe the best way of addressing this is for the government to engage in an ongoing dialogue with industry ***

10. What will be the main drivers of cost to you in supporting lawful interference with communications? Are there any proposals that have been made to you or which you would make that are likely significantly to increase or reduce the costs of lawful interference? For example, would a regime of data preservation (i.e. your retaining data only on suspected persons, which might be several hundred thousand) be significantly cheaper than a universal retention system?

The main drivers of cost for us in supporting lawful interference are:-

- Network and bandwidth growth;
- Manual effort required to support communications data disclosure; and
- Ensuring security of platforms, data and interconnects
- ***

Communications providers must, as under the present regime, be able to recover their costs of setting up and maintaining relevant data retention systems. More generally any increase in the amount data that needs to be retained or in the volume of disclosure requests will tend to increase the costs of the provider. We are already seeing evidence of this in our efforts to comply with current legislation. Also additional cost increases would be caused if the data to be retained is not normally considered or used by the communications provider for its own business purposes.

***

11. How should the government organise its relationship with communication service providers, both when framing legislation on interference with communications, and routinely?

The government should seek to engage communication providers early and throughout any period of legislative development as this will mean the legislator will benefit from maximum exposure to technical expertise and industry knowledge. Communication providers already engage with the government at many levels and on many subjects in this overall area.

There is a concern that the current engagement is fragmented and could therefore benefit from some consolidation to improve information sharing and

reduce providers' cost of dealing with various authorities. Fewer, more technically-skilled points of contact would be desirable in this ever-increasing area of complexity.

12. Is there any other issue relevant to the review's terms of reference that you would like David Anderson to consider? He would find it helpful, were you to set out in as much detail as you can the arrangements for lawful interference with communication that you would prefer to see.

We would make the following remarks:

(i) We believe there is a case for ensuring that legislation for communications data retention/disclosure and lawful intercept be made mandatory to create a level playing field between communication providers. This should include traditional communications providers plus content providers and OTTs.

(ii) There needs to be a framework which explains the purpose, operation and limitations of the legislation and which balances privacy in a fashion that the public understand and accepts as necessary.

(iii) It would be useful if the current legislation could be consolidated to achieve greater transparency and clarity concerning relevant legal requirements ***

(iv) We believe there is a strong case for ensuring that access to communications data is limited to serious crime, terrorism etc. and not used in support of what could objectively be termed less serious crime.

(v) Individual communications providers will for their own business reasons continue to retain certain data types. However if a communications provider retains certain data it can give rise to disclose under the current RIPA. Thus, if different communications providers retain different data, this may result in inconsistent (and potentially unfair) application of the law. This undesirable situation should be addressed in future revisions of RIPA.

(vi) ***

Nick Kelly
Chief Architect
TalkTalk Group
October 2014

Three

I would like to take the opportunity to make a couple of general points before turning to the questions.

First, the importance of open and constructive working relationships between key CSP staff, on the one hand, and Home Office / Law Enforcement Liaison staff, on the other, cannot be understated. Much of what has been achieved since 2000, in terms of an effective police/CSP relationship, is due to constant engagement between individuals who trust each other and who are happy to develop innovative services for the law enforcement community using information that is readily available to CSPs.

It has been my experience that innovative services are developed faster when Home Office liaison officers engage more closely with CSPs. When they engage "at arms length" and when goodwill is stretched, the pace of progress on projects of interest to the Home Office slows.

My experience dealing with law enforcement officials in the Republic of Ireland reminds me of the importance of working with law enforcement officers who engage with the company on a regular basis. The level of technical proficiency of UK SPOCs is considerable, and the willingness of the Home Office to meet reasonable cost-recovery requests has resulted in UK law enforcement officials receiving a service which is of considerable greater quality than similar services provided by CSPs in the Republic of Ireland. None of the answers to the following questions ought to come as a surprise. I expect that, given their very close monitoring of CSP capabilities, the Home Office will be providing your team with briefing materials which make similar points.

1. What are the changes and developments in communications technology, services or methods that need to be taken into account is by the government in framing legislation on interference with communications?

<u>Distinction between services and technology</u>

Until quite recently, there has been a clear delineation between 'traditional' mobile telephony services such as voice and SMS messaging and the more data-centric services such as internet messaging, web browsing, chat rooms, email etc. Each of these service categories have been broadly defined by the technology used to deliver them: circuit- switched in the case of telephony, and packet-switched in the case of data services.

The result of this categorisation has been that CSPs have been the only mainstream providers of telephony services (being the only viable providers of circuit-switched technology) and thus have control over the delivery and usage recording of these services, including the ability to discharge responsibilities under RIPA.

For data services, the case is less clear cut. Whilst CSPs do often provide such services themselves (eg, branded email services), more often than not the only service provide by the CSP is a generic 'data' service, with other

suppliers providing services 'over the top' of this generic data service. In the case of these over the top services, it is highly unlikely that the carrying CSP will have any technical ability to either identify or otherwise control the services being offered in this way. In these cases, the carrying CSP can only discharge their responsibilities under RIPA in terms of the only service that they may provide – a generic data service.

The above becomes a particular issue as data services mature to the point where it is no longer necessary to have a separate circuit-switched technology for the traditional telephony services. Already, there are numerous over the top voice and messaging services such as Skype, Viber etc. More are on the way. CSPs themselves are also at the point of launching traditional telephony services which use the underlying data network as a delivery mechanism, though in this case the. CSP will be able to discharge their RIPA responsibilities.

Because of the above, the legislation needs to make a clearer distinction between the delivery mechanisms (which will always be some form of CSP) and the services which use those delivery mechanisms, many of which the CSPs will have no particular control over or visibility of. It is important to treat CSP and 'service provider·(eg, Google, Yahoo, Viber etc.) equally with respect to RIPA, as it will become increasingly the case that the 'full story' in terms of evidential data will come equally from both sides.

Encryption by default and 'proxy' services

Possibly due to recent press and also as a more general shift in the industry, the end-to- end encryption of services provided over data networks is becoming more prevalent.
Whilst it has always been possible to encrypt services to a degree, most often these features had to be activated by the user and so the take up wasn't as great as might be expected.

The major change is that new services are being released by providers (such as Google) which are encrypted end-to-end by default, and that the user doesn't need to do anything to enable it. Not ·only does this affect communication services such as email, messaging etc., through use of 'proxies', even basic web browsing is starting to become encrypted.

The use of encryption in this way reinforces the fact that the CSP delivering the access mechanisms has less and less visibility or control of the services carried over their networks. The enabler of the encryption mechanisms now need to play a more active role in discharging responsibilities under RIPA.

2. Considering the state of communications technology now and anticipated, does the distinction in existing law and proposed in the draft bill in 2012 betweencommunications data and content continue to be valid? How does this distinction relate to relative intrusion into an individual's privacy?

The distinction between communications data and content can easily blur as a result of using data networks for carrying all forms of communication. For example, services carried over data networks are often 'layered' such that at the most basic layer, only the 2 end points are considered metadata and everything else is content. At a higher layer, more of the 'content' may be considered to be metadata (eg, usernames). At a higher layer still, even more of the content may be considered metadata (eg, dates/times). In other words,

on a technical level, most things can be considered to be content depending on how it is viewed, and how it is viewed usually depends on the role the relevant organisation plays in providing the service.

It is extremely hard for a CSP to comment on the relative degrees of intrusion into an individual's privacy that are implied by the provision by a CSP of content and metadata. Law enforcement investigators are best placed to comment on the quality of the information that can be inferred by metadata.

3. Is the subdivision of communications data into subscriber, use and traffic data appropriate for the future; and are the current definitions of those subdivisions · right? How does this distinction relate to relative intrusion into an individual's privacy?

The definition of subscriber data is reasonably clear, although it is important to bear in mind that, for any given communication, there may be several, possibly different, items of subscriber data for any given party. For example, there may be subscriber data referring to the basic network medium (s) used – mobile *and* WiFi for instance, as well as subscriber data relating to any number of services used to make the communication – email service and private VPN service for instance.

'Use' and 'Traffic' definitions are not always obvious at first sight. Again, distinction needs to be made between the network access mechanism(s) used and the services used via these mechanisms, plus proper recognition that they are likely to come from different sources.

Experience shows that LEAs ·very infrequently request "use data" if traffic data is also
available. It is not clear why these 2 categories should remain separate.

4. How should the government address the challenges to lawful interference with communication that arise from communications services being provided to people in the UK from foreign countries?

Whilst some of the challenges may arise from a -belief in ensuring privacy from the state, it should also be noted that many of the methods being used to ensure this, such as end-to- end encryption and proxying, also prevent CSPs from applying safeguards such as blocking of age-inappropriate, or more seriously, illegal material such as that identified by the Internet Watch Foundation.

The challenges are probably most efficiently met by Home Office officials developing links with the relevant overseas providers that are as robust as those already in place with UK- based CSPs. Alternatively, the challenges can be addressed by better use of other mutual legal assistance arrangements which, while currently in place, are evidently unfit for purpose.

5. How might communications service providers based in the UK be able to assist in lawful interference with communications should overseas-based providers of communications services not cooperate with the British government?

With more pervasive end-to-end encryption of services, this is becoming something that CSPs are less able to assist with. In many cases we are

unable to even identify such services over our own network, let alone exercise any control or detailed monitoring of them.

The answer may, in the end, come from U K based providers who are capable of offering services that are even more compelling than those offered by overseas-based providers.

6. Should the government seek a single international regime for the operation of lawful interference with communications? If so, what might be its principal features?

We have no views on this issue, other than to comment that, given the conflicting views of European Governments who are currently considering issues relating to communications data retention, finding common ground on many aspects of this will prove extremely difficult to achieve. On balance, and in accordance with the subsidiarity principle, it would be preferable for such matters to be resolved at a national level, rather than at a european level.

7. The proposals put forward in 2012 to enable access to communications data depended on certain procedural and technological components, notably the extension of the "single point of contact" and the introduction of the request filter and deep packet inspection. What arrangements would you prefer to see to enable those with lawful authority to obtain communications data or intercept from you and other providers?

We support the proposals relating to the extension of the 'single point of contact'. The current safeguards that form an important component of the SPOC system work extremely well in practice. The statutory oversight of the systems in place to disclose relevant data to those who have a legal duty to demand them is sufficiently robust.

We are not sure whether the proposals for a request filter and deep packet inspection will comprise an effective tool to assist law enforcement investigations. Even where deep packet inspection technology is already used. for business purposes, there is a feeling that it is becoming less widely applicable as many of the over the top services are applying end to end encryption. The logical conclusion is that individual services will eventually become indistinguishable to the carrying CSP.

8. How should the government work with communications service providers to address the impact of the use of encryption on lawful interference with communications, particularly if such use is set to increase?

It needs to be recognized that end-to-end encryption of over the top services is not something that can be controlled by the CSP. International data protection and privacy commissioners increasingly require date in transit to be encrypted, and companies are likely to incur large penalties (in terms of fines and reputational damage) in future if they suffer data breaches involving unencrypted data.

Where it is necessary to either control such services or monitor their use in order to comply with RIPA, this will need to be done by the party employing the encryption

9. What more could be done to exploit the communications data and intercept that is currently available and likely to continue to be so?

It is felt that the data already available is not yet fully exploited, though it is difficult to provide any firm evidence as CSPs do not have full visibility in how it is already used. From experience, however, it does appear to be the case that there are significant variations across the requesting authorities in terms of their ability to exploit the available data. Whilst CSP staff are already engaged to a degree with assisting in this exploitation of available data, an expansion of this could be considered (in the form of additional SPOC training).

10. What will be the main drivers of cost to you in supporting lawful interference with communications? Are there any proposals that have been made to you or which you would make that are likely significantly to increase or reduce the costs of lawful interference? For example, would a regime of data preservation (i.e. your retaining data only on suspected persons, which might be several hundred thousand) be significantly cheaper than a universal retention system?

The cost recovery agreement is paramount to the recovery and co-operation of the UK Communication Service Providers to HMG and must be included in future legislation.

Data volumes are very likely to continue to rise - which will mean a rise in associated costs.

It is difficult to see how a regime of data preservation on 'only suspects' would operate in practice, especially in cases where the retained data may be the only means of actually identifying suspects in the first place (for example, IP addresses associated with criminal communications - potentially every one of our subscribers could have used that IP address at some point in time). Certainly the definition of 'suspect' would ne<td to be very clear and lawfully challenged to prevent any accusation of profiling.

Whilst retained data volumes are likely to increase as a result of an increasing subscriber base, or retention of new data types (such as increased IP address logging), the largest expected cost increases are likely to come from the increasing complexity in the delivery of retained data to the requesting authorities. It is not clear how the Home Office assesses whether all of these delivery mechanisms represent value for money.

11. How should the government organise its relationship with communication service providers, both when framing legislation on interference with communications, and routinely?

There needs to be a recognition that the communications industry is moving at a pace where traditional, prescriptive legislation is always going to significantly lag behind technology and it is not always possible to predict how it will do so. The continuing partnership between HMG and CSPs is essential to ensure that this Jag doesn't develop into a bigger problem.

From a CSPs perspective, there does need to be particular care taken to ensure a level playing field, such that no CSP (including any over the top service provider) is seen to be disadvantaged relative to others by complying

with legislation. Failure to do this could lead to unacceptable commercial outcomes and subsequently Jess willingness on behalf of the CSPs to fully engage.

From a CSPs perspective, there also needs to be particular care taken to ensure that individual CSPs do not maintain relationships with Home Office officials that are perceived to be too close. Misguided and misinformed press speculation could so easily lead to unacceptable commercial outcomes and subsequently less willingness on behalf of the CSPs to fully engage.

My colleagues and I would be delighted to attend meetings to discuss these issues have raised in due course.

Roma Avrili
Information Disclosure Manager
October 2014

UCL

I. Introduction

1. The evidence below is submitted by a group of UCL LLM students of 'Aspects of National Security Law'; a module convened by Dr Tom Hickman (of UCL). It represents the opinions of Daniella Lock, Tara Agoston, Hitesh Dhorajiwala, Josie Teale, Edmund Gross, Edmund Robinson, Aimee Riese, Maryam Siddiqui, Danielle Ralph and Rebecca Wilkinson. It does not represent the views of Dr Tom Hickman.

2. The response is primarily drawn from a series of meetings, organised by class members, about the Investigatory Powers Review. During these meetings we discussed recommendations we would like to make. They are based on observations and commentary arising from class discussion as well as information received from the module's visiting speakers. We also discussed evidence already submitted to the review. Submissions we most engaged with were from the Bingham Centre for the Rule of Law, Liberty and Vodafone.

II. Background

3. University College London Faculty of Laws is the law school of UCL. It is one of UCL's 10 constituent faculties and is based in London. The Faculty was established in 1826 and is a world-famous law school.[1] The LLM offered by UCL involves research-led teaching by experts in their field.

4. 'Aspects of National Security Law' is a course that examines the growth of national security law as an academic discipline. It is concerned with tensions with human rights and the rule of law that occur when seeking to adjudicate national security issues. It is primarily focused on the UK, but has comparative components - particularly in relation to the US, Canada and Australia.

5. The course involves an analysis of the SIAC system, the use of diplomatic assurances, detention, control orders and TPIMs. One of the main focuses of our course has been RIPA powers and the accountability of intelligence services as well as the legal limits to the acquisition and deployment of intelligence.

6. The class has received a number of visiting speakers; all in a unique position to offer insight into national security law in the UK. The speakers include Sir Mark Waller (Intelligence Services Commissioner), Professor Ian Leigh (of Durham University and expert in security services oversight) and Angus McCullough QC (special advocate).

7. Given that the content of our course is highly relevant to material considered within the scope of the Investigatory Powers Review, we felt, despite many of us lacking practical legal experience, eager to contribute our thoughts to the review.

[1] Ranked 4th in Europe 2014 according to QS World University Rankings by subject. See: http://bit.ly/1eoyswH.

Our Submission

8. We recognise that there are multiple threats to national security that this country faces, including those of international terrorism, climate change and financial instability. We also recognise that such threats mean it is vital that the security services are given freedom to protect the interests of national security. For us, the balance must be between this need for freedom and the protection of human rights and the rule of law. It is acknowledged that in certain situations, this may result in privileging secrecy and intrusive surveillance over the fundamental cornerstones of justice, such as due process and the right to privacy.

9. While acknowledging the importance of protecting national security, we welcome the review of investigatory powers by the Independent Reviewer of Terrorism Legislation under Section 7 of the Data Retention and Investigatory Powers Act 2014 (DRIPA). As students of national security law, we can attest to the lack of clarity surrounding certain parts of the law governing this area. This uncertainty runs counter to the rule of law. We also feel there are certain elements of national security law that should be altered to better facilitate the protection of human rights. The Investigatory Powers Review provides much needed occasion to engage with these concerns and consider changes to address them.

III. Legislation Currently Governing Investigatory Powers

10. It is recognised that intercepting communications for the purposes of protecting national security is necessary in some situations. However the law in this area cannot go unchecked. It must also be clear and responsive to changes in technology.

11. In terms of the legal definition of terrorism, we agree with David Anderson's concerns regarding its troubling breadth.[2] Terrorism is recognised as an aspect of 'national security' and the 'interests of national security' is a basis for exercising powers under RIPA. That this definition could potentially result in journalists and bloggers being subjected to investigatory powers as terrorists is deeply concerning. Consequently, we feel there is an urgent need for Parliament to review the definition. We note, with disappointment, that the Counter-Terrorism and Security Bill has not addressed this issue in full.[3]

12. We feel there are also valid concerns regarding the definition of 'national security' more generally. The Council of Europe Commissioner has recently stated that in determining necessity and proportionality of intrusions justified by national security, "the very question of what legitimately can be said to be covered by the concept of "national security" is justiciable".[4]

---

[2] See Chapter 4 of 'The Terrorism Acts in 2012', July 2013.

[3] See David Anderson's comments on page 23 of evidence given to the Joint Committee of Human Rights on 26 November 2014, HC 836

[4] "The Rule of Law on the Internet and in the Wider Digital World", Issue Paper of the Council of Europe Commissioner for Human Rights, 8 December 2014, p 108.

The lack of precision by which national security is defined in the UK means that it is not clear that it is effectively "justiciable". For the Commissioner, matters of national security are "matters that threaten the very fabric and basic institutions of the nation".[5] We would like to point out that this is far narrower than the position taken by the English courts.[6]

13. We acknowledge that flexibility is needed in defining the threats against which investigatory powers can be used. Nonetheless, addressing questions such as the type of threats, and the extent to which more indirect national security interests (for example ensuring good foreign relations with other states), are covered could provide greater clarity. This would ensure a common understanding between the public, the security services and the oversight bodies. In addition, we think that some level of public debate on the appropriate breadth of this concept (rather than the concept being merely a matter for the executive) would provide a clearer and more legitimate basis for the exercise of these powers.

a. RIPA

14. We note that many have already discussed the lack of clarity in regards to the distinction between 'external' and 'internal' communications for the purpose of s8 (1) and s8 (4) intercept warrants in Part 1 Chapter 1 of RIPA.[7] We strongly agree that this distinction is problematic. It has meant that as technology has developed, communication has increasingly been categorised on the basis of chance rather than the nature of the communication itself. Given this, we feel this part of RIPA warrants immediate attention.

b. Surveillance Powers and Ministerial Authorisation

15. In relation to surveillance powers under RIPA, we agree there are potential disadvantages to ministerial authorisation of warrants. Ministers are held to account for failures to protect national security. As such they may be more cautious about protecting national security than an individual's human rights. This might result in more warrants being authorised than are needed and truly justified.

16. To deal with this issue, some have proposed to change the law so that judicial authorisation of warrants is required.[8] However, we feel that the use of judges in both authorisation and review of the granting of warrants is problematic. Following authorisation, judges later reviewing the procedure may be reluctant to criticise the reasoning of a fellow judge.[9] This may undermine judicial capacity to provide effective oversight of warrants once they have been granted. A second concern relates to the extent to which judges have the necessary resources to make decisions in this area. A Minister seems better placed to assess the necessity of a warrant due to the fact that they are able to request further

[5] ibid. p 108.

[6] For example, in Secretary of State for the Home Department v Rehman [2003] 1 AC 153 at para 34.

[7] For example, see paragraph 19 (on page 13) of the Bingham Centre for the Rule of Law Submission.

[8] For example, see paragraph 46 (on page 23) of the Bingham Centre for the Rule of Law Submission.

[9] This was a point made by Profession Ian Leigh during his session with us.

information from the agencies. They also have greater access to resources, in terms of having a bigger team who can provide legal advice and national security expertise. Having studied the ways in which judges decide national security cases, we are not of the view that judicial authorisation would provide a more robust response to the balance of national security and human rights than what is currently in place.

17. We feel the best way to ensure a fair and proportionate balance between these competing interests is to tighten up the review process of warrants once they've expired. Currently, it seems to us that the oversight roles of judges predominantly involves a form of Wednesbury reasonableness review. Much of the process appears to be concerned with whether established procedure has been adhered to, rather than with the substance of decisions made. A more robust form of review might involve a judge and security expert working together to review the merits, including the proportionality question, of the decision to grant the warrant. This would provide greater oversight for the granting of warrants. Additionally, it will not inhibit the process of granting a warrant in moments when flexibility and speed are required.

c. International Cooperation

18. We recognise that the issue of regulating international cooperation between security services, particularly in relation to the exchange of intelligence material resulting from surveillance, is one that brings with it many challenges. We acknowledge that there is particular burden in relation to enacting legal safeguards/international that: a) are effective and b) don't hamper important activities of the security services.

19. Despite the difficulties associated with this issue, we would like to register a concern about the lack of legislation governing international cooperation. As many have noted, the lack of legislation in this area undermines the rule of law. Unchecked cooperation may also bring about human right violations - as we have seen, for example, in the case of *Binyam Mohammed.*[10]

20. We propose that addressing these concerns would also provide opportunity to consider areas for strengthened international co-operation; between UK intelligence services and overseas communications service providers for example.

IV. Oversight

21. In relation to oversight, we recognise that the need for secrecy means it will not always be appropriate to evaluate the substance of decisions made in the interests of national security.

---

[10] See *R (on the application of Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWC

We also acknowledge that in thinking about changes that might be made to the current oversight regime, the availability of resources is a limiting factor.

22. We agree with others that there should be one statutory body responsible for oversight.[11] The way the system currently works is potentially confusing. For those who aren't lawyers it is likely to seem unclear as to who is responsible for overseeing what. The advantage of having one responsible body is that there would be greater clarity for the general public as to who is in charge of (and therefore accountable for) reviewing the activities of the security services.

23. If the function of already existing oversight bodies is retained, we think changes should be implemented to ensure increased communication between them. In particular, there should be greater dialogue between the Commissioners. That there is currently no joined up approach between them means that they may often review decisions relating to the same operation but are each unable to benefit from the other Commissioner's work.

a. The Commissioners

24. We think the Commissioners should review the substance of a greater proportion of executive decision-making. For example, in relation to the authorisation of interception warrants, we think that the Intelligence Services Commissioner should be responsible for evaluating the merit of reasons given for authorization.[12]

25. We acknowledge that there are advantages of having individuals, with highly respected professional positions, probe security service activities. However we are concerned about the relationship of trust such individuals might feel they need with the security services in order to do their job effectively. The felt necessity of such a relationship may serve to discourage Commissioners from being critical of the security services. Given this concern, we feel there should be more openness surrounding the relationships the Commissioners have with the security services.[13]

b. The Intelligence and Security Committee (ISC)

26. We welcome the fact that the ISC are now holding certain evidence-gathering sessions in public and publishing reports with greater frequency. The increased level of detail they contain about activities of the security services are also welcomed.

---

[11] For example, see paragraph 46 (on page 23) of the Bingham Centre for the Rule of Law Submission.

[12] One modification that might address this concern is that each Commissioner (possessing, as they do, extensive and highly valuable judicial expertise) would be supplemented by two colleagues. At least one of these individuals would be required to possess detailed knowledge and experience of national security; for example, a former member of the security services or senior diplomat. This would in effect create a panel modelled loosely on the SIAC bench. This wider field of expertise would be better able to undertake substantive review of decisions.

[13] For examples, by introducing a statutory requirement that all meetings the Commissioner have are recorded and made publicly available (including any that might happen out of working hours).

27. We note the increase in media appearances by members of the ISC. Such appearances help to make the oversight regime more accessible to the general public. However, we feel it should be emphasised that these media appearances are not a substitute for greater transparency regarding the substantive elements of the ISC's work.

28. Following the Justice and Security Act 2013, the ISC has statutory footing as a Parliamentary Committee. We are concerned that this change means the ISC no longer qualifies as a 'public authority' for the purposes of Section 6 of the Human Rights Act 1998 (HRA).[14] We think there that the ISC's status in this regard should be made explicit. If it is the case that the ISC no longer qualifies as a 'public authority' for the purposes of the Human Rights Act 1998, then a new statutory requirement should be introduced to ensure it is brought within the scope of the Act.

29. We also think a specific requirement should be introduced to ensure that the ISC assesses the extent to which the security services comply with human rights generally. Such a requirement would necessitate a suitably staffed legal advisory team to assist the ISC. When dealing with issues of human rights, it is crucial that a) the ISC has the specific statutory requirement to provide oversight on human rights compliance and b) that it has the expertise to be able to provide rigorous legal scrutiny in this regard.

30. We would like to add that the ISC's most recent report on Lee Rigby Fuslier was a point of contention within our class. Some questioned the idea that communication services providers (CSPs) were providing 'safe havens' for terrorists.[15] It was felt that evidence regarding the sharing of information with the Kenyan security services was by far the most significant issue to be discussed in the report. In light of this, some saw the prominence given to the role of internet companies, in commentary made by the ISC to the media, as politically motivated.[16] Others, however, felt there was significant force in the ISC's statements regarding CSPs. It was felt that this is a legitimate area of concern, particularly as CSPs have increasing numbers of users and advanced technology. According to such members of the class, there is evidence to suggest that terrorist organisations are increasingly developing a firm understanding of how CSPs work and using them on a large scale worldwide. On this basis, certain members of the class felt that access to this information derived from CSPs could be vital for Counter-Terrorism.

c. The Civil Courts and the Security Services

31. We are concerned that the use of closed material procedures (CMPs) in the civil courts have been used with greater frequency than might have been expected. The government claimed that CMPs have

---

[14] See: Ian Leigh 'Balancing Rights and National Security' p727.

[15] Intelligence and Security Committee of Parliament, 'Report on the intelligence relating to the murder of Fusilier Lee Rigby', Chair: The Rt. Hon. Sir Malcolm Rifkind, MP, 25 November 2014, paragraph 19.

[16] See article: Sir Malcom Rifkind, 'Lee Rigby murder: It was preventable, but an internet company failed to alert the authorities', Daily Telegraph, 25 November 2014.

only been used 'sparingly' since the Justice and Security Act 2013 came into force. However, recent research suggests that CMPs are being used in a wide variety of cases.[17]

d. The Investigatory Powers Tribunal (IPT)

32. The IPT is the only domestic forum where the public can make human rights complaints about unlawful surveillance. As such, we think it is of concern that the Tribunal should be subject to an ouster clause that precludes any further domestic scrutiny of its decisions (except to the extent that the Secretary of State orders otherwise).[18] [19] We find this state of affairs troubling considering that in the last decade of its operation, the IPT has upheld a total of 10 complaints, resulting in a success rate of 0.5%.[20] [21]

33. We are also concerned by rule 6 (1) of the IPT Rules 2000. Under this rule, the IPT may prevent the disclosure of evidence that may act in any way "contrary to the public interest or prejudicial to national security". The fact that this is not balanced against concerns of open justice creates a system of disclosure unduly weighted in favour of the government. This only emphasised by the fact that the IPT must seek the consent of the security services before disclosing information. Such a state of affairs seems contrary to dicta given in *Binyam Mohamed*. In this case, Lord Neuberger stated that while significant weight must be given to the reasons given by the executive for not disclosing information, the final arbiter must be a court; a position we are inclined to agree with.[22]

34. We would like to add that the recent decision of the IPT in *Liberty* has also been a cause for concern for members within our class. Of particular unease is the IPT's conclusion that although the nature of contemporary communications data has blurred the distinction between internal and external communications, the distinction as maintained in RIPA remains relevant and unambiguous. In the opinion of the IPT, this means RIPA is compatible with Article 8 of the ECHR.[23] However, we would be inclined to disagree with this conclusion. As discussed above, we agree with those that emphasise the increased complexity of the nature of communications data transmission. We think the internal/external distinction has lost much of its purpose, and may have the potential to allow circumvention of RIPA through the choice of classification of intercept data (a problem the IPT acknowledged).[24]

---

17 See recent report by the Bingham Centre for the Rule of law on the use of CMPs under the Justice and Security Act 2013.

18 See Section 67(8) of RIPA.

19 This point has been expanded upon by Bernard Keenan, LSE, in a recent talk on the IPT given on the 8 December 2014.

20 See JUSTICE, *Freedom from Suspicion* at para 358; 5 of these 10 successful complaints arose from the same case.

21 Though we do accept that the scope for appeal is severely limited regardless of the clause - due to decisions of 'No Determination in Favour of Complainant' not being accompanied by reasoning.

22 *R (Mohamed) v Secretary of State for Foreign and Commonwealth Affairs (No 2) (Guardian News and Media Ltd and others intervening)* [2010] EWCA Civ 158; [2011] QB 218 [131] – [132] (Lord Neuberger MR).

23 See *Liberty and Others v GCHQ* [2014] UKIPTrib 13_77-H at para 100.

24 Ibid. para 53.

Concluding Remarks

35. Thank you for taking the time to read this submission. In our opinion, national security law should always strive to be clear and protect human rights. We very much hope the Investigatory Powers Review can be used to ensure this.

January 2015

Vodafone

The evidence below details Vodafone's background as an international communications company before examining the significant change in the communications landscape since the turn of the century, and in particular the introduction of the Regulation of Investigatory Powers Act 2000. Notwithstanding these changes, Vodafone remains committed to supporting the legitimate efforts of law enforcement and intelligence agencies in tackling serious crime, terrorism and threats to national security.

The evidence builds on Vodafone's recently published Law Enforcement Disclosure Report and addresses the key subjects of current and future technologies, the implications for the legal framework of the changing global nature of technology and Vodafone's view that surveillance[1] powers must be considered in the wider context of other powers and capabilities. In particular Vodafone would like to emphasise the need to ensure obligations are applied appropriately and fairly across all members of the communications sector, not just telecommunications operators, and the imperative of full cost recovery for the services used.

All of the above must be considered within the context of the subject of privacy and human rights; the one word we consider to be the bedrock of our business is trust. The evidence focuses on the principles of legitimacy, necessity and proportionality while reflecting on the need for Government accountability and transparency.

Finally, Vodafone would like to see a broad and full review of all relevant legislation with the objective of consolidating it under a single framework with strong approval and oversight procedures.

1. Background on Vodafone

1.1 Vodafone is an international communications company, offering fixed line, mobile and IP-based communications services to Europe, the Middle East, Africa and Asia Pacific.[2] Vodafone is also one of the world's leading providers of M2M[3] services, the enabler for the so called Internet of Things, and provides cloud, hosting and application services for both consumers and enterprises worldwide.

1.2 Trust is the bedrock of our business and our business model. Correspondingly, respect for our customers' privacy is paramount. If our customers begin to believe that their personal communications are no longer private, they will either use our services less or switch to others they believe are more protective of their privacy. While generalised concerns and awareness about privacy do not necessarily translate directly into these behaviours, in highly competitive markets such as the UK even small shifts in sentiment can have significant consequences. When customers have to make finely balanced decisions about which service provider to give their business to, trust becomes a tipping factor in the decision to move to another operator, to use a different app, associate with a different brand, and so on.

[1] We use the term 'surveillance' generically to cover the monitoring, intercepting, collecting, obtaining, analysing, using, preserving, retaining, interfering with, accessing or similar actions taken with regard to information about a person's communications

[2] http://www.vodafone .com/content/index/about/about-us/where.html

[3] For a brief explanation of M2M, visit: http://m2m.vodafone.com/cs/m2m/discover-m2m/what-is-m2m?column=1&nav=1&row=1

1.3 It is also a matter of fact and of serious consideration for us that government surveillance requirements can significantly impact the efficient running of our business. For instance, the requirement to implement complex technical capabilities creates not just significant operational costs, but creates complexities that influence architectural decisions in the way we deploy networks and services, as well as slow down how quickly we are able to launch products and respond to market developments and competitive pressures. This is accentuated when those pressures come from companies not encumbered by the same legal requirements, either because they are not recognised as providing telecommunications services, or because they are established in other countries with little corporate presence in the UK.

1.4 We do, however, recognise the importance of legitimate and lawfully authorised communications surveillance in supporting the efforts of law enforcement and intelligence agencies in tackling serious crime, terrorism and threats to national security. Conducted within a clear legal framework that is fit for purpose and subject to the rule of law, few would seriously question why this is essential in maintaining our nation's security, the safety of British citizens and in protecting the freedoms that are essential to our society.

2. Vodafone and law enforcement assistance

2.1. There are various pieces of legislation that impact Vodafone today[4], however it is the Regulation of Investigatory Powers Act 2000 (RIPA) that has the greatest impact since it is the instrument through which the vast majority of law enforcement and intelligence agency demands are received by Vodafone.

2.2 RIPA was introduced following decisions[5] by the European Court of Human Rights highlighting deficiencies in the UK for the interception of communications. This background is significant, because RIPA sought to provide a comprehensive legal framework for the use of a variety of investigatory powers that was consistent with the European human rights framework.

2.3 However the world has changed since 2000:

- Extreme terrorism: The 9/11 attacks on the US, followed by the attacks in Madrid and London, heralded a new era for the US, the UK[6] and our allies in focusing intelligence and national security efforts at tackling the threat of extreme terrorism. The physical, as well as the psychological, impact of these attacks should not be under-estimated, and has served to shape much of the political debate about security over the last decade. This has directly impacted citizens (increased security at airports being one of the most visible consequences) and businesses (for the telecoms sector,
- the introduction of data retention legislation being a direct result; for the airlines, the introduction of Passenger Name Records disclosure to the US authorities, to name a

[4]Data Retention and Investigatory Powers Act 2014, Communications Act 2003 and wider communications legislation, Privacy and Electronic Communications Regulations 2003, Regulation of Investigatory Powers Act 2000, Enterprise Act 2002

[5]Further information can be found on the ECHR's website:
http://www.echr.coe.inUDocuments/FS_Data_ ENG.pdf

[6]Leading Prime Minister Tony Blair to declare after the London bombings in 2005 "the rules of the game are changing"

couple of obvious examples).

- The Snowden revelations: the Snowden revelations have caused another sea- change in public perception and awareness, although perhaps those revelations are still too recent for us fully to understand the longer term implications. But the fact of this review, and the review instigated by President Obama last year, is a clear indication that public attitudes have changed, and the government approach to the conduct of surveillance needs to change with it.

- Technological change: The way we communicate has altered radically since the late 1990s. In 2000, mobile phone penetration stood at a mere 12% of the population worldwide[7]. The number of internet users worldwide was estimated at 361 million[8], less than a third of the users on Facebook today. Google was just over a year old. There were no such things as smart-phones, mobile apps or social media. Communications services were provided almost exclusively by nationally licensed/ authorised telecoms service providers, who would typically also operate the underlying physical network, i.e. voice and text services were indistinguishable from the underlying carriage service. All of the capabilities of those networks - the relevant access network, the switches and routers, billing and application platforms where customer data would be processed - would typically be physically hosted within the same country. Cloud based communications didn't exist, and webmail service providers had just begun to offer alternatives to client-based email solutions.

- By 2014, mobile penetration has surpassed 95% worldwide, and internet users exceed 2.8 billion people[9]. More significantly, the availability of communications options has mushroomed - most importantly, the provision of access and connectivity has been decoupled from the services people use to share, communicate, store and access information. The availability of open platforms and smart-phones, coupled with higher bandwidth mobile and fixed networks, has enabled these 'over-the-top' services to grow rapidly, as they often require little infrastructure, there are low barriers to entry, including an absence of regulatory constraints (such as licensing or authorisation), and can be provided from almost anywhere in the world.

These changes have successively and simultaneously:

- heightened fears about safety and the ability to detect and prevent potential terrorist attacks, particularly as terrorists become adept technologists themselves;
- raised new fears about the legitimacy of government surveillance, both by domestic agencies and those overseas, opening a fresh debate on whether the balance between intrusion into individual freedoms and the protection of those same freedoms ;
- caused intelligence agencies to have serious concerns that technology is causing the internet to 'go dark' and thereby hamper attempts to tackle extreme threats; while also raising hopes by others that technology can provide a new frontier of freedom from the excessive (and in some cases oppressive) state control on communication and freedom of speech and association by authoritarian regimes.

2.4 We recognise that there is now a strong and urgent need for reform to maintain trust in law enforcement/intelligence activities, and in communication service providers who are subjected to legal duties to provide assistance. The legal powers relied upon by agencies and authorities must be fit for the digital age.

[7] ITU World Communications/ICT Indicators (WTI) database
[8] Internet World Stats: http://www.internetworldstats.com/stats.htm
[9] Internet World Stats: http//www.internetworldstats.com/stats.htm

2.5 The UK has long been a leader in democracy and civil liberties and has both a leadership role and a responsibility in setting the framework for the future. We should, in particular, be mindful that other countries will watch closely what we do.

2.6 We note that the scope of the review refers only to "investigatory powers", rather than a broader review of legislation pertaining to the surveillance of communications. We think it vital, however, to consider the broader principles behind the issues and as such we recently published our Law Enforcement Principles. We believe these principles address the key issues and as part of this submission we thought it would be helpful to summarise clearly how we believe Governments should approach these issues, as below.

3. Vodafone's Law Enforcement Principles

3.1 In our view, regardless of the country, legislative frameworks empowering government agencies to conduct surveillance must be:

- tightly targeted to achieve specific public protection aims, with powers limited to those agencies and authorities for whom lawful access to customer data is essential rather than desirable;
- proportionate in scope and defined by what is necessary to protect the public, not by what is technically possible; and
- operationally robust and effective, reflecting the fact that households access the internet via multiple devices - from games consoles and TVs to laptops, tablets and smartphones - and each individual can have multiple online accounts and identities.

3.2 We also believe that Governments should:

- balance national security and law enforcement objectives against the state's obligation to protect the human rights of all individuals;
- require all relevant agencies and authorities to submit to regular scrutiny by an independent authority empowered to make public - and remedy - any concerns identified;
- enhance accountability by informing those served with demands of the identity of the relevant official who authorised a demand and by providing a rapid and effective legal mechanism for operators and other companies to challenge an unlawfulor disproportionate demand;
- amend legislation which enables agencies and authorities to access an operator's communications infrastructure without the knowledge and direct control of the operator, and take steps to discourage agencies and authorities from seeking direct access to an operator's communications infrastructure without a lawful mandate;
- seek to increase their citizens' understanding of the public protection activities undertaken on their behalf by communicating the scope and intent of the legal powers enabling agencies and authorities to access customer data; and
- publish regular updates of the aggregate number of agency and authority demands issued each year or at the least allow operators to publish this information without risk of sanction.

4. Current and future threats, capability requirements and the challenges of current and future technologies

There are a number of significant trends taking place that will be critical in shaping the framework for investigatory powers. While we list these as four separate areas, they are naturally interconnected

4.1 Communications technology and the economic and business landscape will continue to change rapidly

- New types of IP-based communications will continue to emerge, along with new forms of networks for carrying those communications. Services and networks will become increasingly de-coupled, and even networks may become de-centralised, e.g. mesh networks, and ad-hoc user controlled networks using Bluetooth and other forms of Near-Field Communication[10].
- Conversely, cost pressures will cause existing network operators to look for efficient network structures, such as sharing core network capabilities across a number of markets, and potentially outside the UK[11].
- These changes will test the effectiveness of traditional investigatory powers that require the assistance of communications service providers, founded on the basis of corporate entities established in the UK, providing end to end communications services on UK based infrastructure.

4.2 The business and technology landscape will continue to become more global, while the regulation of law enforcement and national security activities remain national

- As service and cloud providers are able to reach markets without a physical presence in the UK (infrastructure or personnel), often data relating to communications or other activities will be hosted outside of the UK, making this data potentially inaccessible to UK agencies, but conversely accessible to the agencies of the countries where the providers are located or where the data is hosted[12].
- Where the laws of those countries do not provide equivalent protection for non-residents or citizens, or even lower levels of protection (e.g. the US, where the law only provides protections to US persons, leaving non-US persons without protection[13]), this poses risks to UK Citizens the protection of whose right to privacy and freedom of expression effectively passes outside UK jurisdiction. Conversely, UK based providers will be able to serve markets overseas, which could - without adequate legal safeguards - make data belonging to people with no connection to the UK available to UK

[10] In recent protests in Hong Kong, protesters have resorted to using a mesh networking application, FireChat, in order to bypass Chinese government censorship and potential disablement of cellular networks. This mesh network technology does not require any centralised cellular or Wifi network: http: //www. extremetech.com/extreme/191118-hong-kong-protesters -turn-to-mesh -networks-to-evade-chinas-censorship

[11] Vodafone has consolidated parts of its core messaging infrastructure. In particular, in 2010, Vodafone's Greek unit consolidated its SMSC infrastructure with Vodafone' s Italian business unit, hosted in Italy. However, following the adoption into Greek law of the Data Retention Directive, Vodafone Greece was forced to repatriate the infrastructure to Greece, due to restrictions in the law on generating traffic outside of the territory of Greece. Vodafone has avoided locating some of its UK servers outside the UK due to legal compliance concerns related to law enforcement access.

[12] Microsoft is currently fighting legal action brought by US government agencies seeking disclosure of data from its Hotmail servers in Ireland, arguing that US law does not and should not allow a warrant to be effected outside the territory of the US - http://www.theguardian.com/technology/2014/sep/03/microsoft-contempty-court-judge-data-dispute

[13] Report to European Parliament, 2013 "US Surveillance programmes and their impact on EU citizens' fundamental rights" - http://www..europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL- LIBE_NT{2013)474405_EN.pdf

intelligence and security agencies, even where the communication concerned has no connection to the UK other than the UK being the corporate seat of the service provider.

- The low cost of market entry for many new providers means that the number of players in the market will greatly expand, and they will be able to set up quickly in places with the least regulation. These entities are likely to be less willing (and able) to cooperate with UK law enforcement agencies, even if UK law can, lawfully, be given extra-territorial effect.

4.3 Ever greater volumes of data about an ever widening range of human activities (not just communications) will be generated as more objects become digitised and connected, using M2M technologies in the Internet of Things

- The vast and ever growing pool of data about people's communications and other digital activities, coupled with advancing data analytics capabilities, will provide both private actors and government agencies with insights that were previously unknowable. Just as "Big Data" is mooted to be a catalyst for transforming health care, transport and many other essential services, it has the capability to transform government intelligence and surveillance. Consequently, the opportunities for surveillance and intelligence gathering, whether lawful or otherwise, are likely to grow exponentially.
- In due course, the intelligence value of this data may far surpass the existing value of techniques, such as interception of communications content. However, unlike interception of communications content, the acquisition of Big Data may be conducted piecemeal, from a myriad range of providers and sources, with no single source being easy to identify as particularly intrusive, and therefore necessitating higher safeguards.

4.4 Privacy and cyber security fears and concerns will continue to rise in the public consciousness

- This is likely to be driven both by attempts by policy makers and regulators to update legal frameworks for data protection / privacy and raise standards among the private and public sector, but also the continuing fallout of the Snowden revelations and the perceived excesses of government surveillance.
- This in turn, will likely continue to drive market responses to these changing attitudes[14], including the provision of specialist secure devices[15], encrypted personal clouds[16] and communications, and encrypted network connections by default[17]. One particular consequence of significance is that some providers will seek to place the means for decryption out of their own hands (where they can otherwise be legally required to decrypt communications on demand) and directly into the hands of their users or customers, or other 'trusted third parties'.

5. The implications for the legal framework of the changing global nature of technology

[14] While there are many examples of how the market has responded to consumer concerns about abuse of their personal data (such as this report from Ovum: http: //www.ovum.com/biq-trust-is-big-datas-missing-dna/), the most recent and high profile example was provide by Apple's Tim Cook http://bqr.com/2014/09/18/tim-cook-on-apple-provacy-2/)

[15] For example: Blackphone, produced by Silent Circle and Geeksphone - https://www.blackphone.ch/

[16] For example: Paoga, a UK start up - http://www.paoga.com/

[17] For example: Google is introducing encryption by default for all traffic from its Chrome Browser – http://dev.chromium.org/spdy/spdy-whitepaper

5.1 Ensuring a comprehensive legal regime

- An effective regime for enabling law enforcement and intelligence agencies to gain lawful and legitimate access to communications and data must recognise that it cannot focus obligations of assistance on particular classes of provider but must find mechanisms to address the whole of the communications sector. Otherwise, the regime will be asymmetric, negatively impacting domestically established companies over other classes of provider, while at the same time being ineffective in achieving its aims.
- It must also address the global nature of the challenge - both in providing law enforcement and intelligence agencies with lawful and legitimate access to information that is essential to their task, but also in protecting and safeguarding the rights of citizens. The solution to this must be diplomatic, at least with the UK's major trading partners and allies, and we welcome the appointment of Sir Nigel Sheinwald as the Prime Minister's Special Envoy. However, we believe the terms of reference should include an express objective to ensure the reciprocal protection of the rights of citizens by the US and other key international partners.
- We also note that given the EU discussions around the notion of a "connected continent", there is an obvious need to remove territorial restrictions caused by legislation. A connected continent will require a level of international cooperation and alignment within EU member states that doesn't exist today.

5.2 Key principles

Surveillance powers need to be looked at holistically in light of other powers and capabilities:

- Policy makers should not start from the position that 'what went before must therefore continue in the future'. The powers that were appropriate in the 1990s are not necessarily the right powers in the far more advanced and complex world of today.
- For example, while the value of real-time interception may be reducing as new forms of 'over-the-top' communications become harder to monitor by law enforcement authorities, there has correspondingly been a massive expansion and proliferation of data sources, such as geo-location data, imaging and sensing data, with corresponding techniques for data mining and analytics, that provides law enforcement authorities with powerful new forms of intelligence and insight.

Surveillance powers must be business and technology-neutral:

- The legitimacy of surveillance powers is undermined if they are ineffective at achieving their stated aims, or are easily circumvented by those they seek to monitor or observe. For example, if the powers are limited to particular technologies that can be circumvented through the use of alternatives, or that quickly become outdated by fast-paced technological advance, this limits the effectiveness of such powers while also creating an unfair burden and commercial disadvantage for service providers using 'regulated' technologies.
- Surveillance powers, and the requirements on communications service providers or operators to provide assistance, should therefore address the types of services provided, and not the business models or underlying technologies used to provide them.

6. The safeguards to protect privacy

6.1 We believe national security and law enforcement goals must be conducted within a framework that respects human rights. To the extent possible, the goals of national security and law enforcement must be made to be consistent with the protection of human rights. Only where they come into inevitable conflict must a balance be struck between them.

6.2 It is essential to Vodafone that trust is rebuilt in the role of Government agencies and

companies in carrying out legitimate and lawfully authorised surveillance activities. Achieving that depends both on having an up-to-date and fit-for-purpose legal framework based on clear principles, but also on public visibility that the framework is operating appropriately and effectively. Accordingly, there are a number of principles that we believe are essential to safeguarding privacy:

6.3 The scope and use of surveillance powers must be subject to the principles of legitimacy, necessity and proportionality

- Surveillance powers should only be used for legitimate purposes, namely to tackle serious crime and terrorism, and to protect national security and public safety.
- Surveillance powers should only be available where they are necessary to achieve their ends, i.e. considering all the circumstances, there are no other appropriate means of tackling serious crime or protecting national security or public safety.
- Any use of powers must be proportionate to the threat that a government agency or law enforcement authority is seeking to address. In particular, surveillance powers should be targeted at particular individuals or at specific events or threats based on clear and justifiable grounds, not conducted on a blanket basis across populations.

6.4 Governments should be subject to laws governing downstream use and management of data

- In addition to restrictions on the right to conduct surveillance and access data, government agencies should be subjected to laws governing their subsequent use of data and intelligence. In particular, there should be clear requirements limiting the retention of data for only so long as necessary for the intelligence or law enforcement purpose for which it was lawfully obtained.

6.5 Governments and their agents must be accountable for their use of such powers

- The use of surveillance powers must only be permitted following lawfully authorised prior approval and independent oversight mechanisms.The rule of law requires that any executive interference with an individual's rights should be subject to effective control. These controls should guarantee independence, impartiality and respect for proper procedure.
- The level of prior approval, and the standard required to be met, should be appropriate and proportionate to the seriousness of the threat at issue. In particular, for the most intrusive surveillance powers, such as communications content interception, real-time location tracking or the amassing of large volumes of data across multiple sources, we believe Parliament should debate the potential role of judicial authorisation.
- In order to minimise the risk of undermining public support for the use of surveillance powers for legitimate national security and public safety purposes, the use of surveillance powers should be limited to a defined set of law enforcement or intelligence agencies that are tasked with tackling serious crime, terrorism or the protection of national security and public safety (as per section 7.1 of this evidence, below).
- The internal government process to request and/or authorise an order should:
    - set out the facts and grounds that justify the order (although certain facts may be subject to national secrecy restrictions, and only available to appropriately cleared individuals on a need-to-know basis)
    - demonstrate the relevance and necessity of the surveillance power requested to address a specified threat
    - identify the government official who authorised the application for, or granting of, the order
- Orders issued to communications service providers to provide assistance should be made in writing, should state clearly what is required to be done by the provider (but not how it should be done) and by when, should state clearly what lawful power is being

invoked, identify the official who requested or made the order and , where applicable, identify the judge who made the order[18]

- In order to ensure that legal powers are not being misused or misconstrued , it is essential that the legal foundation for the use of powers is made publicly available. While this must not enable operational information that would compromise law enforcement or intelligence activities, it should enable the use of powers to be challenged before the courts and thereby enable clarification of the law. This clarification in the context of an adversarial process will provide an essential tool for Parliament to exercise oversight and determine whether the law is continuing to operate as was intended, or whether amendments are needed.

6.6 We believe there are certain statistical and transparency requirements that should apply:

- Transparency, in terms of the publication of statistical information relating to the requests by law enforcement and others, is an important mechanism to allow a greater understanding of the volume of such requests. Vodafone published its first law enforcement disclosure report[19] in 2014, which included the publication of statistics on access to communications data and on the provision of lawful interception services. Where a country's government published its own statistics, Vodafone included or referenced these and, in respect of other countries, where not legally prohibited, Vodafone published its own figures.
- In our view, it is governments - not communications providers - who hold the primary duty to provide greater transparency on the number of agency and authority demands they issue. We believe this for two reasons.

    - First, no individual provider can provide a full picture of the extent of agency and authority demands across the country as a whole, nor will a provider understand the context of the investigations generating those demands. It is important to capture and disclose demands issued to all providers, and individual providers may not be willing to invest the resource in producing and publishing such figures.
    - Second, different providers are likely to have widely differing approaches to recording and reporting the same statistical information. Some providers may report the number of individual demands received, whereas others may report the cumulative number of targeted accounts, communications services, devices or subscribers (or a varying mixture of all four) for their own operations. Similarly, multiple different legal powers may be invoked to gain access to a single customer's communications data: this could legitimately be recorded and disclosed as either multiple separate demands, or one.
- To add to the potential for confusion, an agency or authority might issue the same demand to five different providers; each provider would record and disclose the demand it received in its own way; and the cumulative number of all providers' disclosures would bear little resemblance to the fact of a single demand from one agency.
- In our view, inconsistent publication of statistical information by individual providers amounts to an inadequate and unsustainable foundation for true transparency and public insight. There is a substantial risk that the combination of widely varying methodologies between providers (leading to effectively irreconcilable raw numbers) and the potential for selective withholding of certain categories of agency and authority demand (for reasons which may not themselves be fully transparent) would

[18] In exceptional and urgent cases where life is at risk, it may be necessary and proportionate to use expedited procedures. Where that is the case, the correct process must be completed as soon as possible, to ensure that there remains a full account of the basis upon which the power was used.

[19] http://www.vodafone.com/contenUsustainabilityreport/2014/index/operating-responsibly/privacy and security/lawenforcement.html

act as a significant barrier to the kind of meaningful disclosure sought by the public in an increasing number of countries.

- We believe that regulators, parliaments or governments will always have a far more accurate view of the activities of agencies and authorities than any one provider. However, our belief is not without qualification. In order for publication of this statistical information by the authorities to be meaningful and reliable, in our view it must:

    - be independently scrutinised, challenged and verified prior to publication;
    - clearly explain the methodology used in recording and auditing the aggregate demand volumes disclosed;
    - encompass all categories of demand, or, where this is not the case, clearly explain those categories which are excluded together with an explanation of the rationale supporting their exclusion; and
    - encompass demands issued to all providers within the jurisdiction in question.

- We believe that the approach of the Interception of Communications Commissioner in his most recent report is consistent with these principles, and Vodafone would support the publication of these figures in each future report.
- However, we do question whether the Interception of Communications Commissioner has the resources and expertise to conduct the tasks of his/her office with sufficient rigor bearing in mind the size and sophistication of law enforcement and intelligence gathering. Parliament needs to ensure that the powers and resources for providing oversight remain under review and sufficient for the task at hand.

6.7 Rights of appeal, review and redress

- There should be a power to appeal to the most senior court on the legality of any order, and courts must have power to order a review of the use of surveillance powers and provide redress.
- In particular, service providers must be able to appeal against an order to provide assistance, including the development of technical capabilities.

7. The case for amending or replacing the legislation

7.1 Consolidate the laws under which surveillance demands can be made

- In 2013, Vodafone conducted a non-exhaustive analysis of statutory powers in the United Kingdom which could be interpreted as giving powers to various agents of government and law enforcement to require a communications company to hand over data including communications data. This turned up approximately 40 pieces of legislation.
- Vodafone considers that the approach promulgated by the Data Retention and Investigatory Powers Act 2014, at s6, which seems to limit the scope of powers under which communications data can be acquired, to be a very positive step. A consolidated legal framework, incorporating sufficient approval and oversight procedures, is the most suitable mechanism for authorising demands for assistance with communications surveillance.

7.2 Vodafone and, we assume, other service providers are increasingly being placed in positions where they have to make complex decisions about demands for assistance with law enforcement or intelligence from government agencies, e.g. whether specific technical capabilities have to be designed into new networks, services or other technologies being deployed. The law, however, is far from clear because technology has moved on apace. The law therefore lacks the quality required of it by the European Court of Human Rights, which is unacceptable when fundamental rights are at stake.

8. Government should bear the reasonable costs of surveillance

8.1 The costs, in terms of both CAPEX and OPEX, associated with technical compliance with law enforcement demands, can be significant. The full cost of surveillance assistance by communication service providers should be borne by the government as it is fulfilling the state's duty to protect citizens, and is otherwise an interference with the lawful use by a communications service provider of its assets and property. If costs are allowed to fall disproportionately on certain market players like network operators, this will inevitably influence the competitive dynamics of the market and ultimately the type and nature of services provided by different players.

8.2 Requiring government to bear the cost of surveillance both acts as a sensible restraint on the potential for excessive use of surveillance powers and also contributes to accountability by ensuring that the financial impact of surveillance is apparent, and not hidden in sunk costs borne by industry.

For further information:

Guy Matthews
Senior Government Affairs Manager