Investigatory Powers Review

Written submissions (A-G)

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.

Access

Table of Contents

Introduction

Access welcomes the opportunity to submit evidence to the Investigatory Powers Review, and to inform Parliament's continuing work on this crucial area of law and regulation.

In our submission, we recommend that Parliament consider its laws and policies related to communications surveillance, specifically in regards to the impacts on fundamental human rights of internet and telecommunications users. The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles"),[1] which provide a framework for assessing states' human rights duties and obligations when conducting surveillance, are particularly instructive in this regard. The Principles, which Access helped to draft, have been endorsed by more than 400 civil society organizations around the world. The landmark 2014 report by the UN High Commissioner of Human Rights Navi Pillay acknowledged that the Principles can serve as interpretive guidance of Article 17 of the International Covenant on Civil and Political Rights.[2]

Long legacies of the exercise of free expression, privacy, and other civil and political rights in the UK should continue into the digital age. Fortuitously, digital rights protections also benefit innovation and the information economy, and will ensure that international businesses and users see the UK as a safe, secure place to conduct online activity and commerce.

Diverse stakeholders have labored to strengthen global standards on transparency and privacy, and now seek more uniform implementation in domestic law to protect human rights and increase accountability worldwide. The UK can play strong role in this effort by reforming its

[1] https://en.necessaryandproportionate.org/text.
[2] OHCHR, *The Right to Privacy in the Digital Age*, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

surveillance legislation to protect rights online as they are offline, for its citizens and users around the world. To achieve these goals, we urge greater transparency on the government's surveillance activities; critical review of data retention mandates for consistency with international law and norms; and principled vigilance on any government interference with cryptographic standards.

1) Increasing Trust and Certainty

One year after the release of the International Principles on the Application of Human Rights to Government Surveillance, secrecy continues in the UK and elsewhere through overbroad laws, judicial and legislative gag orders, and threats of retaliation for disclosures. Silence on the scope and scale of government surveillance leaves users in the dark, harms the reputations of private companies, and destroys trust and certainty in the information economy. In the UK, especially, secret courts and policies restricting the reporting and disclosures deter from efforts to inform citizens on the extent of surveillance online.

States and service providers both have rights and responsibilities regarding transparency on communications surveillance. Governments should pursue both the active role of keeping users informed of the processing and transfer of their personal data, as well as the more passive role in recognizing the right of providers to do the same.

Moreover, providers often say that "transparency is the government's responsibility." On surveillance, they maintain, governments are better positioned to disclose surveillance practices than the businesses processing their requests. For their part, governments must loosen restrictions and disclose data on their own activities, including in national security.

Transparency Reports, beyond the numbers

At their best, "transparency reports" can reveal the scope and scale of surveillance online. Generally, they include aggregate statistics of requests that governments issue for user data, giving details like the type of request, why it was issued, and whether the recipient complied. They're one of the proactive ways that companies, governments -- really any entity dealing with user data -- can directly inform users about risks to their communications and other activities online.

Governments have made some progress on transparency. Earlier this year, the U.S. government reached a settlement[3] with major internet platforms allowing them to release aggregate data on certain national security requests. Companies have upheld their end of the bargain, as more and more firms adhere to the government's strict guidelines and report national security requests for the first time. Yet companies eager to regain the trust of users still push for more transparency: the U.S. government imposed a delay on acknowledging Foreign Intelligence Surveillance Court (FISC) orders, and only allows statistical reporting in bands of

[3] WSJ, *Government Reaches Deal With Tech Firms on Data Requests*, http://online.wsj.com/news/articles/SB10001424052702303277704579347130452335684.

several hundred.[4] Elsewhere, various governments and departments have succeeded in engaging the public with open data policies. In Hong Kong, government statistics come alive through the skillful visualization and helpful explanations in the Hong Kong Transparency Report.[5]

To date, however, most States have lagged far behind of internet and telecommunication providers when it comes to reporting on their surveillance activity. Ironically, it took a private service provider, UK-based Vodafone, to reveal the legal and operational context of government surveillance -- and just how much we don't know.[6] Out of 29 countries where Vodafone does business, governments in 8 either bar disclosure of surveillance requests, or were, at the time of the report, too unstable to even approach with the question, according to the company. In 10 countries, Vodafone's report marked the first time any entity, either provider or government, had published surveillance data. Another handful of states enjoy direct access to the company's networks, leaving the provider, and users, no idea of the extent of surveillance and the corresponding interference with user rights taking place.

In the U.S., the bulk of communications metadata collected still falls into a legal black hole. The DOJ settlement did not allow reporting on the number of customer accounts affected by FISA Section 215 orders, which require telecom providers to deliver metadata of daily call records, affecting millions of users.[7] The U.S. intelligence directorate's own transparency report similarly lacked rigor and clarity[8] on the scale and scope of government surveillance, falling short of the granularity that the "We Need to Know Coalition" - a multistakeholder group including companies like Google and Microsoft, NGOs including Access, CDT, and the ACLU, and trade associations - has identified as necessary.[9]

UK Transparency

The UK has shown some foresight on transparency, creating the Interception of Communications Commissioner's Office with the passage of RIPA in 2000. This Office publishes statistical information on lawful interception and communications data demands issued by agencies and authorities. While its 2013 report[10] provided greater detail than previous releases, the Commissioner's reports have been broadly criticized as lacking in scrutiny, failing to break down surveillance requests into granular categories, and being critically circumscribed in scope.

[4] Twitter, *Fighting for more transparency*, https://blog.twitter.com/2014/fighting-for-more-transparency
[5] Hong Kong Transparency Report, http://transparency.jmsc.hku.hk.
[6] Vodafone, *Law Enforcement Disclosure Report*, http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf.
[7] https://www.techdirt.com/articles/20140127/17253826014/feds-reach-settlement-with-internet-companies-allowing-them-to-report-not-nearly-enough-details-surveillance-efforts.shtml
[8] https://www.accessnow.org/blog/2014/06/27/us-intelligence-report-misses-opportunity-for-openness
[9] Access, *We Need to Know: Companies, Civil Society Call for Transparency on Surveillance*, https://www.accessnow.org/blog/2013/07/18/tech-companies-and-civil-society-join-call-on-the-us-government-to-issue-tr.
[10] IOCCO, *Annual Report of the Interception of Communications Commissioner* (2013), http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf.

In the UK, according to Vodafone,

> Section 19 of the Regulation of Investigatory Powers Act 2000 prohibits disclosing the existence of any lawful interception warrant and the existence of any requirement to provide assistance in relation to a warrant. This duty of secrecy extends to all matters relating to warranted lawful interception. Data relating to lawful interception warrants cannot be published. Accordingly, to publish aggregate statistics would be to disclose the existence of one or more lawful interception warrants.[11]

Of particular interest to foreign users, the Commissioner cannot report on the number of certificates and warrants issued under Section 8(4) of RIPA, which allows for the interception of the content of communications via a certified warrant.[12] A Section 8(4) warrant "does not have to name or describe one person as the interception subject or a single set of premises as the target of the interception,"[13] according to the Commissioner, which allows its use for mass surveillance purposes. The Section 8(4) warrants "are restricted to the interception of external communications … sent or received outside of the British Islands."[14] In other words, the law targets foreign communications, directly implicating the human rights to privacy and free expression of users around the world.

Additionally, any acknowledgement of UK programs that allow police or intelligence services direct access to networks, or instances thereof, are missing from the Commissioner's reports. For instance, GCHQ conducts mass surveillance via satellites and fibre-optic undersea cables, scooping up huge volumes of data from communications between innocent people.[15] And Vodafone found that Section 5 of the Intelligence Services Act 1994 ("ISA") could grant powers "broad enough to permit government direct access to Vodafone's network by the Security Services in some instances."[16] Neither of these powers are detailed by the Commissioner.

Two-way accountability

Transparency is the first step toward accountability on UK surveillance activities, which impact millions of individuals on a daily basis. Recipients of lawful intercept warrants should be able to acknowledge and report them. As transparency reporting by businesses fast becomes a global

[11] Vodafone, *Law Enforcement Disclosure Report*, http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf, at pg. 77.
[12] See Statewatch, *Analysis*, at http://cryptome.org/2014/05/gchq-lawful-world-spy.pdf.
[13] *See supra* note 8, at 8.
[14] *Id*.
[15] Guardian, *Mastering the Internet: How GCHQ Set Out to Spy on the World Wide Web*, http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet; Guardian, *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[16] Under this law, "the Secretary of State may, on an application made by the Security Service, the Intelligence Services or GCHQ, issue a warrant in respect of any property so specified or in respect of wireless telegraphy." *See supra* note 6, at 86.

business standard, the international community will continue to demand greater trust and certainty in UK firms as a prerequisite to trade and transfer of data across borders.[17]

For its part, the Interception of Communications Commissioner should be greatly empowered to count and question the government's wide ranging surveillance activities, with statistics broken down by agency and accounting for surveillance of foreigners.

Where both companies and governments issue transparency reports, users benefit most: two-way accountability will increase as the reports converge toward uniform standards on counting and reporting individual requests. The checks and balances these reports can provide on statistics and context help to ensure the UK public -- and foreign users -- are adequately informed about communications surveillance, and able to participate in robust debate on its proper limits.

Surveillance courts and transparent law

Secret law and secret courts do not yield legitimacy or accountability. Access supports massive changes to the U.S. Foreign Intelligence Surveillance Court (FISC), and similar calls to reform the UK's Investigatory Powers Tribunal (IPT), as both forums lack the open and adversarial processes necessary to produce legitimate law or accountable practices in accordance with international human rights standards.[18]

On the U.S. side, the publication of some court opinions has provided valuable information on the extent of government surveillance -- and bolstered calls to make public many more opinions. The opinions revealed that a "special advocate" is needed to counter the government's arguments.[19] The U.S. President's Review Group on Intelligence and Communications Technologies suggested the special advocate be summoned on the discretion of the FISC judge, ostensibly for cases with novel questions or with wide-reaching impact.[20] Under the Review Group's recommendations, the special advocate would also receive docket information and be allowed to join the proceedings on their own initiative (without an invitation).

The UK IPT similarly must undergo reform of its procedures and judgments. Rather than increasing the number of secret hearings, as has been proposed,[21] the IPT should empower the subjects of surveillance with notice of pending complaints, and constant representation by the court's special advocates. The court should publish its opinions, open decisions to judicial

[17] To this end, Access and our partners have called providers like BT, who do not currently issue transparency reports, to begin doing so immediately. See https://www.accessnow.org/blog/2014/07/18/bt-no-transparency-report-in-the-foreseeable-future.
[18] *Don't Spy on Us: Reforming Surveillance in the UK*, https://www.openrightsgroup.org/assets/files/pdfs/reports/DSOU_Reforming_surveillance.pdf
[19] See Access, *Structural Changes to Surveillance Court Offer Hope for New Protections for Non-US Users*, https://www.accessnow.org/blog/2014/01/24/structural-changes-to-surveillance-court-offer-hope-for-new-protections-for, for a delineation of the powers this advocate should carry.
[20] http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf%20
[21] Guardian, *Ken Clarke Warned Plan to Curb Open Justice is Flawed*, http://www.theguardian.com/politics/2012/jan/08/ken-clarke-curb-open-justice-flawed.

review and appeals, and proceed with the presumption that cases be held in open forums, by default.

These U.S. and UK surveillance court reforms are necessary, but far from sufficient, to reform the perception of rubber-stamp surveillance authorities that routinely fail to provide effective remedy for users at risk.

2) Data Retention: Disproportionate, Unnecessary, and Costly

Blanket data retention increases risks and costs to companies and users, while turning all citizens into suspects. We submit evidence that the U.S. government has sent mixed signals on the utility of data retention for surveillance purposes, while domestic and international jurists have not been so forgiving.

U.S. law and regulations

Lacking a mandatory data retention law in the U.S.,[22] the NSA enforces de facto data retention of U.S. telephony data by holding onto the call detail records (CDRs) it bulk collects from telcos under requests made pursuant to Section 215 of the USA Patriot Act. There are some limits to this retention: since at least 2006, the Foreign Intelligence Surveillance Court (FISC) has told the NSA to destroy these records after five years.[23] In January 2014, this requirement was codified in FISC Judge Reggie Walton's Primary Order as one of several safeguards, or "minimization procedures."[24] Incredibly, the NSA fought even this modest restriction, but lost in court last March.[25]

In his ruling against the NSA's motion to extend retention periods, Judge Walton found that extending the time limit on data retention under Section 215 of the USA Patriot Act "would further infringe on the privacy interests of United States persons."[26] The judgment noted that data retention "increases the risk that information about United States persons may be improperly used or disseminated," especially considering that "the great majority of these individuals have never been the subject of investigation" for intelligence purposes. Data retention lobs a hugely disproportionate impact onto unsuspecting citizens.

[22] An FCC regulation adopted in 1986, 47 CFR 42.6 (http://www.law.cornell.edu/cfr/text/47/42.6), does require telephone companies to retain toll call billing records for eighteen months. This scope of the regulation includes toll call subscriber and call metadata, defined as "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call." Yet this does not include many types of data transmission and users of contract phone plans.
[23] *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, BR 06-08 (FISA Ct. 2014) , http://www.dni.gov/files/documents/11714/FISC%20Order,%20BR%2006-08.pdf.
[24] DNI, *Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program*, http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/994-foreign-intelligence-surveillance-court-approves-government%E2%80%99s-application-to-renew-telephony-metadata-program.
[25] TechDirt, *DOJ Asks To Hang Onto Bulk Collections Longer, Citing Need To 'Preserve' Evidence It Has No Intention Of Presenting In Court*, https://www.techdirt.com/articles/20140227/08464126374/doj-asks-to-hang-onto-bulk-collections-longer-citing-need-to-preserve-evidence-it-has-no-intention-presenting-court.shtml.
[26] *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, BR-1401 (FISA Ct. 2014), http://www.emptywheel.net/wp-content/uploads/2014/03/14-01_Opinion.pdf.

Even U.S. intelligence authorities have dithered on data retention's necessity and utility. In 2006, the Department of Justice did not press the FCC to extend the retention period established twenty years earlier.[27] The NSA terminated its email metadata program in 2011.[28] And recently, both the Attorney General and the Director of National Intelligence conceded that the intelligence community does not need a data retention mandate. They argued that the current version of the USA FREEDOM Act, a surveillance reform bill lacking data retention requirements, "will accommodate operational needs while providing appropriate privacy protections."[29]

CJEU ruling and UK law

The spring 2014 ruling by the Court of Justice of the EU ("CJEU") also puts into question the lawfulness of blanket data retention in general.

On April 8, 2014, the Grand Chamber of the European Court of Justice ("CJEU") invalidated the EU Data Retention Directive, holding that it exceeded the bounds of the EU Charter, specifically in regard to the principle of proportionality as to the Directive's interference with the rights to privacy and data protection as set out in Articles 7 and 8.[30] Adopted by the European Union in 2006, the Data Retention Directive mandated that all telecommunications data - including mobile and landline phones, fax, and email - are to be indiscriminately collected and retained by providers for a minimum period of six months, and up to two years.[31]

To implement the Directive, the UK passed Regulations in 2009 requiring that communications data "generated or processed in connection with the provision of publicly available electronic communications services or public communications networks" be retained for a period of twelve months.[32] The invalidation of the Directive had the substantive impact of nullifying the UK Regulations and similar laws in other EU member states.[33] Despite this, the Minister of State for Immigration at the Home Office explained in May that it was of the view that "the UK Data Retention Regulations … remain in force."[34]

[27] EmptyWheel, *The White Paper's Selective Forgetting on FCC Phone Record Retention History*, http://www.emptywheel.net/2013/08/11/the-white-papers-selective-forgetting-on-fcc-phone-record-retention-history.
[28] Guardian, *NSA Collected US Email Records in Bulk for More than Two Years Under Obama*, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama
[29] Letter from Eric Holder, Attorney General, and James Clapper, Dir. Nat'l Intelligence, to Patrick Leahy, Sen. (Sept. 2, 2014), http://images.politico.com/global/2014/09/04/clapperholderleahyltr.pdf.
[30] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051;%20http://europeanlawblog.eu/?p=2289
[31] Access, *A Closer Look at EU Court's Ruling and What it Means for the Future of Data Retention in Europe*, https://www.accessnow.org/blog/2014/04/11/a-closer-look-at-eu-courts-ruling-and-what-it-means-for-the-future-of-data.
[32] http://www.legislation.gov.uk/uksi/2009/859/pdfs/uksi_20090859_en.pdf
[33] http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Briefing-on-the-Data-Retention-and-Investigatory-Powers-Bill.pdf
[34] http://www.theyworkforyou.com/wrans/?id=2014-06-16c.199250.h&s=%28%22we+consider+that%22%29+speaker%3A11640#g199250.r0

The CJEU ruling is decisive, highlighting the need for, at the very least, greater public debate on mandatory data retention and mass surveillance, given its adverse, unnecessary, and disproportionate impacts on fundamental rights. Yet on July 10, 2014, three months after the Directive was invalidated, the Data Retention and Investigatory Powers Act (DRIP)[35] was introduced in the UK Parliament as emergency legislation. The bill's proponents did not leave adequate time for democratic processes to take hold and shape the proposed rules. Alarmingly, the DRIP was considered under "emergency" or "fast track" procedures, which greatly diminish the public involvement and the time available for debate or consideration of alternative proposals. Instead of using established process,[36] the UK Government bypassed established procedures in order to not only retain its previous authority, but to greatly expand the UK surveillance state.

By its terms, the DRIP not only re-enacts the previous Regulation, without attempting to conform to the CJEU judgment, but also grants significant new authority to "extend the territorial scope of the broad interception and communications acquisition powers under the [Regulation of Investigatory Powers Act 2000 ("RIPA")]." In practice, this will open up companies to increased obligations to retain and share data with the UK government and impede on the rights of users around the world.

In the wake of the CJEU ruling, Finland[37] and Luxembourg[38] have already announced that their national laws on data retention would be reviewed. The DRIP runs contrary to the CJEU's April judgment as well as international law and established human rights principles. In line with the Charter of Fundamental Rights of the EU, any restrictions on fundamental rights are to be subject to the principle of necessity and proportionality.[39] All surveillance programs and authorities should be demonstrably necessary, proportionate, and transparent, and "data retention or collection should never be required of service providers."[40]

High costs

Along with creating lucrative targets for malicious actors,[41] data retention mandates pose significant costs. Telecom executives have voiced concerns over standardizing their datasets to match government needs.[42] Datasets would have to be held well beyond their business purpose,[43] creating significant liability risks and negative externalities: a company's international

[35] https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill
[36] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/328408/Guide_to_Making_Legislation_July_2014.pdf
[37] http://www.helsinkitimes.fi/finland/finland-news/domestic/10120-finland-must-revise-its-data-protection-laws.html
[38] http://www.gouvernement.lu/3641093/08-cjue
[39] http://www.europarl.europa.eu/charter/pdf/text_en.pdf
[40] https://en.necessaryandproportionate.org/text
[41] Nigel Brew, *Telecommunications Data Retention-An Overview*, PARLIAMENT OF AUSTL. DEP'T OF PARLIAMENTARY SERV. (Oct. 24, 2012), http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/1998792/upload_binary/1998792.pdf.
[42] Marcy Gordon & Martha Mendoza, *AT&T, Verizon And Sprint Push Back Against The NSA, Too*, THE HUFF. POST (Mar. 3, 2014), http://www.huffingtonpost.com/2014/03/03/att-verizon-sprint-nsa_n_4891533.html
[43] *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security of the Comm. on the Judiciary*, 112th Cong. (2011) (statement of Kate Dean, U.S. Internet Serv. Provider Assoc.).

reputation would suffer for its association with domestic surveillance regimes,[44] while its energy-wasting datacenters contribute to environmental harms.[45] Ultimately, these costs are passed on to users, hampering economic growth and innovation while reducing the global competitiveness of domestic platforms and networks.

Data retention causes adverse impacts on human rights and economic innovation, while increasing data insecurity. The UK must repeal its mandates, and allow companies to minimize data retention. After all, "Data destroyed cannot be misused."[46]

3) Benefits of Strong Cryptography

Access believes the Independent Reviewer should take this opportunity to study the participation of UK government authorities in the creation, maintenance, and dissemination of cryptographic standards and tools.

The "Integrity" Principle of the International Principles on the Application of Human Rights to Communications Surveillance offers guidance:

> In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems… .[47]

Any interference with general-use encryption standards not intended solely to correct vulnerabilities or otherwise increase the strength thereof is a facial violation of the Integrity Principle. Similarly, any failure to disclose known vulnerabilities in algorithms to be immediately patched is likewise a violation.

Though common now, this type of interference by governments did not always occur. Previously, a nation's enemies communicated in secret codes that only they knew, and that only they used — you might say it was an early example of proprietary software. So when states attempted to crack one another's communications, they used their own cryptographic experts who worked to crack the code of their enemies, but did not interfere with communications of the general public.

However, today, encrypted digital communications are typically built upon the same open protocols, whether they are sent by an intelligence agency, a major corporation, or an ordinary

[44] *Foreign Intelligence Surveillance Act (FISA) Reforms: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. (2014) (statement of Michael Woods, Vice President and Assoc. Gen. Counsel, Verizon Commc'ns).
[45] James Glans, *Power, Pollution, and the Internet*, N.Y. TIMES (Sept. 22, 2012), http://www.nytimes.com/2012/09/23/technology/data-centers-waste-vast-amounts-of-energy-belying-industry-image.html
[46] James Plummer, *Data Retention: Costly Outsourced Surveillance,* CATO INST. (Jan. 22, 2007), http://www.cato.org/publications/techknowledge/data-retention-costly-outsourced-surveillance.
[47] https://necessaryandproportionate.org/

user. Vulnerabilities in the security of one of these standards exposes all other stakeholders using the same protocol. In this way, weaknesses in encryption algorithms are akin to “back doors” into software, programs, and databases. The problem is, even if you trust without reservation the entity building that back door for its own use, these doors are also exploitable by other actors, be it overreaching governments, authoritarian regimes, or unaffiliated bad actors.

Encryption algorithms form the foundation of a secure internet, which in turn is the basis for personal communications and social networking, e-commerce and banking, news consumption, academic research, and just about every other major use of the internet. It is therefore important to make sure that they are as strong and secure as possible.

The UK should ensure that there is separation between entities developing cryptographic standards, and those empowered with the mandate to uncover threats to national security. In short, keep your lock-makers away from your lock-breakers.[48] To this point, Access organized a recent coalition letter signed by 30 companies and organizations and 5 noted technical experts, including Eleanor Saitta and Jacob Appelbaum.[49] The missive specifically explained that governments should empower a civilian agency to perform the “information assurance” functions, of helping to defend information systems, rather than leaving the lock-breakers in charge.[50]

Any country that works on information assurance should empower such an agency and keep it independent from any other agency that serves any surveillance function. The independent agency should receive its own adequate funding and resources. In addition, the agency should be empowered with sufficient technical expertise to allow it to operate on its own discretion rather than depending on other experts, like a life preserver, in order to serve its established function. Until governments institute changes like these, it is unlikely that users will be able to fully trust much of the internet’s infrastructure, and or feel truly secure in the privacy of their personal transactions.

Conclusion

The UK Parliament must carry out several essential reforms to regain its leadership on civil and political rights protections. Transparency from the government and by companies carrying out surveillance requests is key to communicating risks and rebuilding the trust of users in the businesses that hold their sensitive data. Data retention mandates violate fundamental human rights, and threaten the global competitiveness of UK firms, for no proven security benefit, and must be abolished. Finally, attention to cryptographic standards and the integrity of systems will ensure that all users remain secure and free to exercise their rights online.

[48] See https://www.accessnow.org/blog/2014/09/18/virtual-integrity-the-importance-of-building-strong-cryptographic-standards for recommendations to US government authorities regarding cryptographic standards and safeguards.
[49] https://www.accessnow.org/page/-/Veto-CISA-Coalition-Ltr.pdf
[50] See https://www.accessnow.org/blog/2014/04/21/access-and-partners-call-on-nist-to-strengthen-cryptography-standards

In conclusion, Access reiterates our support for the Independent Reviewer's work and our intention to guide the Investigatory Powers Review toward effective and immediate outcomes for users at risk, worldwide.

***

Access (AccessNow.org) is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information, please contact:
Peter Micek
Senior Policy Counsel
peter@accessnow.org

October 2014

Link to submission: https://www.accessnow.org/blog/2014/10/15/access-contributes-to-independent-review-of-uk-surveillance-abuses

SUBMISSION TO THE HOME OFFICE'S CONSULTATION ON THE INTERCEPTION OF COMMUNICATIONS CODE OF PRACTICE FROM THE APPG ON DRONES

INTRODUCTION

1. This submission is concerned with the Home Office's proposed amendments to the existing Interception of Communications Code of Practice ('the Code'). The Officers of the All Party Parliamentary Group on Drones ('the APPG') welcome the opportunity to provide input into the Code on behalf of the APPG. The APPG has a particular interest in the interception of communications as a preliminary step in the gathering and use of intelligence to facilitate lethal drone strikes, and the legal and human rights implications thereof.

2. The APPG notes the publication during the consultation period of a major report by the Intelligence and Security Committee of Parliament ('the ISC Report').[1] The ISC Report recommends that the current statutory framework – including the Regulation of Investigatory Powers Act 2000 ('RIPA') – be repealed and overhauled by one single, comprehensive statute setting out clearly the powers of the intelligence and security agencies and the safeguards on the exercise of those powers. Clearly if this course of action were to be pursued the Code might become redundant. However, it is likely that many of the issues raised in the course of this consultation would ultimately require attention in the drafting of a new bill: this makes the consultation a useful exercise in any event.

BACKGROUND

3. In January 2014 the APPG Chair, Tom Watson MP, sought independent advice from barristers Jemima Stratford QC and Tim Johnston on the lawfulness of five assumed scenarios concerning the interception of communications. The advice set out five key conclusions:

    a. The bulk interception of external communications – *i.e.* communications sent or received outside the British Islands – was lawful under RIPA but likely to amount to a disproportionate interference with the privacy rights of those affected under Article 8 of the European Convention on Human Rights ('the ECHR').

    b. The statutory safeguards with regard to the retention, use and destruction of communications data (also known as metadata) and external communications were insufficiently stringent, and also likely to violate Article 8 ECHR.

    c. The Secretary of State had a wide and largely unrestrained discretion to permit the transfer of intercepted communications to foreign powers. This unfettered discretion was incompatible with the requirements of the ECHR.

[1] '*Privacy and Security: A Modern And Transparent Legal Framework'*, March 2015, available at http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf.

d. The transfer of data to foreign powers, in the knowledge that they were likely to be used to facilitate drone strikes against non-combatants, was probably unlawful and could, at least in theory, give rise to criminal liability on the part of those individuals involved.

4. A copy of the advice is attached as Annex 1.[2] The advice has previously been submitted on behalf of the APPG to the Intelligence and Security Committee ('ISC') and the Royal United Services Institute, and was referred to in the APPG's responses to two prior consultations – the Home Office's consultation on the Covert Surveillance Code of Practice[3] and the Information Commissioner's Office's consultation on the CCTV Code of Practice.[4]
    a. The bulk interception of external communications – *i.e.* communications sent or received outside the British Islands – was lawful under RIPA but likely to amount to a disproportionate interference with the privacy rights of those affected under Article 8 of the European Convention on Human Rights ('the ECHR').

    b. The statutory safeguards with regard to the retention, use and destruction of communications data (also known as metadata) and external communications were insufficiently stringent, and also likely to violate Article 8 ECHR.

    c. The Secretary of State had a wide and largely unrestrained discretion to permit the transfer of intercepted communications to foreign powers. This unfettered discretion was incompatible with the requirements of the ECHR.

    d. The transfer of data to foreign powers, in the knowledge that they were likely to be used to facilitate drone strikes against non-combatants, was probably unlawful and could, at least in theory, give rise to criminal liability on the part of those individuals involved.

5. A copy of the advice is attached as Annex 1.[5] The advice has previously been submitted on behalf of the APPG to the Intelligence and Security Committee ('ISC') and the Royal United Services Institute, and was referred to in the APPG's responses to two prior consultations – the Home Office's consultation on the Covert Surveillance Code of Practice[6] and the Information Commissioner's Office's consultation on the CCTV Code of Practice.[7]

6. In addition, following correspondence with Professor Sir David Omand, the authors of the

[2] Also available at: http://appgdrones.org.uk/wp-content/uploads/2014/08/APPG_Final_advice.pdf. The scenarios, whilst assumed for the purposes of the advice, were based on news reports of the Edward Snowden leaks.
[3] http://appgdrones.org.uk/wp-content/uploads/2014/08/SUBMISSION-TO-THE-HOME-OFFICEfinal262.pdf
[4] http://appgdrones.org.uk/wp-content/uploads/2014/08/SUBMISSION-TO-THE-ICO-FINAL-26-6-2-3.pdf
[5] Also available at: http://appgdrones.org.uk/wp-content/uploads/2014/08/APPG_Final_advice.pdf. The scenarios, whilst assumed for the purposes of the advice, were based on news reports of the Edward Snowden leaks.
[6] http://appgdrones.org.uk/wp-content/uploads/2014/08/SUBMISSION-TO-THE-HOME-OFFICEfinal262.pdf
[7] http://appgdrones.org.uk/wp-content/uploads/2014/08/SUBMISSION-TO-THE-ICO-FINAL-26-6-2-3.pdf

advice prepared a supplementary note, attached as Annex 2.[8]

7. The Home Office will also be aware of the important judgments of the Investigatory Powers Tribunal ('IPT') in the actions brought by Liberty, Privacy International *et. al.*, which were published on 5 December 2014 and 6 February 2015. Those judgments held that the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, obtained by US authorities, contravened Articles 8 or 10 ECHR, but that following disclosures made in the course of the hearings themselves the violations had come to an end.

8. Finally, the APPG notes that two of its officers, Chair Tom Watson MP and Vice-Chair David Davis MP, have brought proceedings against the Home Secretary seeking a declaration that section 1 of the Data Retention and Investigatory Powers Act 2014 ('DRIP') is incompatible with Article 8 ECHR and Articles 7 and 8 of the European Union Charter of Fundamental Rights, in the light of the decision of the Court of Justice of the European Union in the *Digital Rights Ireland* case.[9] Mr. Watson and Mr. Davis have brought this action in their individual capacities as Members of Parliament, not on behalf of the APPG. However, in light of the ongoing proceedings, this submission will not address any amendments to the Code arising from DRIP.[10]

9. The issue of interception of communications has given rise to concerns amongst many Members of Parliament over the last year, as well as amongst the leading human rights NGOs, including Liberty, Privacy International, Big Brother Watch, Open Rights Group and Reprieve.[11] An Early Day Motion on the subject of state surveillance, tabled by Mr. Watson MP in June 2014, was signed by 43 Members of Parliament.[12]

LIMITS TO CONSULTATION

10. As a preliminary matter, the APPG notes that the Home Office does not seem to have made available a version of the new Code that 'tracks' or otherwise shows clearly the changes made to the previous draft. The unintended consequence may be that small but potentially significant changes to the Code pass unnoticed. For example, para 4.6 of the previous version of the Code – which deals with urgent authorisation of section 8(1) warrant – states that "*an urgent case is one in which interception authorisation is required within a twenty four hour period*". The equivalent para 5.6 of the new Code omits that sentence, with the result that the concept of an "*urgent*" case does not appear to be defined in the new Code. As the ISC Report highlights, transparency concerning the limits and safeguards that apply to the intrusive powers given to security and intelligence agencies is essential. In the interests of transparency, the APPG suggests that in future all proposed changes to those safeguards be

[8] The APPG is grateful to Professor Sir David Omand for agreeing to disclosure of this note.
[9] Joined Cases C-293/12 and C-594/12.
[10] For the avoidance of doubt, this submission is made by the Officers in their capacity as Officers of the APPG, on behalf of the APPG and without prejudice to any evidence or submissions made in Mr. Watson and Mr. Davis's claim against the Home Secretary.
[11] See Liberty brief to Independent Reviewer of Terrorism Legislation
[12] Available at: http://www.parliament.uk/edm/2014-15/147.

identified as clearly as possible.

11. In a broad sense, the focus of the Code is on clarification of the statutory safeguards already in place rather than substantive improvement of those safeguards. In other words, the consultation exercise proceeds on the basis that the overarching regulatory framework is lawful and adequate. It is not clear that this is true. Public consultations, required under existing statutory provisions, are no substitute for a comprehensive review of RIPA and the six other Acts of Parliament that apply to intrusive capabilities: the Security Service Act 1989; the Intelligence Services Act 1992, the Wireless Telegraphy Act 2006; the Telecommunications Act 1984; the Counter-Terrorism Act 2008; and DRIP.

THE DRONES CONTEXT

12. The APPG's primary concern with the Code is its failure to consider (or consider adequately) the sharing and end-use of intercepted data by a foreign state.

13. As summarised by Jemima Stratford QC and Tim Johnston, the current position under RIPA is as follows:

    a. Subsections 15(2) and 15(3) of RIPA limit the number of persons to whom intercepted communications (and related metadata) may be disclosed, and the extent to which the data are disclosed, to the minimum necessary for the authorised purposes.

    b. However, subsection 15(6) lifts those requirements in relation to communications and metadata shared with foreign countries.

    c. In respect of data transferred overseas, the Secretary of State has a wide discretion to decide whether requirements corresponding to those in subsections 15(2) and 15(3) need apply and, if so, to what extent.

    d. The Secretary of State also has discretion to decide whether restrictions need be in place to prevent the disclosure of the intercepted material in a foreign court and, if so, to what extent.

14. As the supplementary note by Ms. Stratford and Mr. Johnston clarifies, the Intelligence Services Act 1994 also provides (at section 4) that the Director of GCHQ must ensure that GCHQ does not disclose any information except so far as necessary for the proper discharge of its functions (or for the purpose of criminal proceedings). Section 2 imposes a similar duty on the Chief of the Intelligence Service. Section 2 of the Security Service Act 1989 imposes substantially the same obligation on the Director-General of the Security Service.

15. Finally, Ms. Stratford and Mr. Johnston point out that section 15 of RIPA is only expressed to apply to data (and related metadata) acquired under warrants. RIPA sets out a different scheme for the interception of pure metadata; this does not require a warrant, merely an 'authorisation' (section 22). There is an ambiguity in RIPA as to whether the disclosure of metadata obtained under an authorisation to a foreign power is allowed at all; but if it is, it does not appear to be subject to any restrictions or safeguards at all.

16. At the international level, APPG understands that the exchange of communications intelligence derived from foreign communications (i.e. communications of foreign countries) between the UK and the USA is governed by a multilateral agreement dating back to 1946 ('the UKUSA Agreement'). The full text of the UKUSA Agreement was disclosed in 2010 on the NSA website; it is possible that related documents, such as subsidiary arrangements, may remain secret.[13] The UKUSA Agreement contains only limited safeguards on the use of such intelligence, e.g. prohibiting its dissemination to entities that will exploit it for commercial purposes. The default position is that the exchange of intelligence will be "*unrestricted*" *[…] except when specifically excluded*". Art 3(b) provides:

    It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon.

17. The APPG acknowledges the undoubted importance of intelligence-sharing but expresses concern at the virtually unfettered discretion that appears to be given to the Secretary of State and the security and intelligence agencies in this respect.

18. The disclosure to a foreign power of data relating to an individual is a significant interference with the Article 8 rights of that individual. Interferences with Article 8 are only permissible where they are necessary for one of several specified purposes (e.g. national security) and proportionate to that aim. An interference will not be proportionate if it is not 'in accordance with the law'; it is well-established that proportionality requires, at an absolute minimum, clear and foreseeable limits on the exercise of any executive power to interfere with rights (see e.g. *Malone v UK*[14]).

19. In the *Liberty* IPT case, the Tribunal held:

    > *41 … We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute … or even in a code … It is in our judgment sufficient that:*
    > *(i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it (as per* Malone*…)*
    > *(ii) They are subject to proper oversight.*

20. The IPT's judgment (and, similarly, the ISC Report) focuses primarily on the receipt of shared intelligence from the US by UK agencies. Neither looks in any depth at the current arrangements for sending intelligence data overseas. However, it is clear that - even by the IPT's modified standard set out above – the arrangements for the disclosure of data to foreign powers by UK agencies are not adequate for the following reasons.

21. First, the Secretary of State has a wide statutory discretion under RIPA to determine what safeguards, if any, must be applied to intercepted communications disclosed to foreign powers. Neither the Code nor any other public document constrains the exercise of this

[13] I. Brown and D. Korff, '*Foreign Surveillance: Law and Practice in a Global Digital Environment*', [2014] EHRLR 243, fn 39.
[14] European Court of Human Rights, application no. 8691/79.

discretion.

22. Second, despite a written request from members of the APPG to the Foreign Secretary, the internal guidance on the passing of communications data by UK intelligence and security agencies to foreign powers has not been disclosed.[15] The failure to disclose relevant internal guidance was a significant factor in the IPT's finding of a violation of Art 8 and/or Art 10 in the *Liberty* case.[16]

23. Third, the UKUSA Agreement provides no meaningful safeguards on the sharing of intelligence data. The UKUSA Agreement was clearly drafted at a time when official state communications were more readily intercepted than the private communications of individuals. That distinction is no longer relevant. The default position under the Agreement is that intelligence will be shared save in exceptional circumstances; that is not compatible with the modern concept of proportionality. Finally, and in any event, it is not clear whether the Agreement applies to internal communications (as defined in RIPA) or the communications of private individuals at all; yet section 15(6) of RIPA clearly envisages that such communications might be shared with foreign powers.

24. For those reasons, it is very likely that the current framework relating to the sharing of communications intelligence fails the proportionality test.

25. The position is even more worrying in relation to metadata acquired under a section 22 authorisation, as there seem to be no limits at all on the sharing of such information (bar the broad requirements in sections 2 and 4 of the Intelligence Services Act 1994 and section 2 of the Security Service Act that any disclosure be necessary for the discharge of the agencies' functions).

26. Insofar as a policy choice has been made to exempt metadata from the (very limited) safeguards of section 15 of RIPA, the APPG disagrees with this approach. The APPG does not accept that disclosure of metadata is somehow more benign than disclosure of the contents of communications. Recent technological advances have largely elided the significance of the distinction between contents data and metadata. A great deal of highly sensitive information can be gleaned from metadata: as Liberty has put it, metadata paints "*a rich picture of what a person does, thinks, with whom, when and where*".[17]

27. US National Security Agency ('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.[18]

[15] Available at: http://appgdrones.org.uk/wp-content/uploads/2014/08/Rt-Hon-Philip-Hammond-MP9-FINAL-3.pdf.
[16] Both the IPT Judgments and the ISC Report make reference to the existence of internal guidance on the *receipt* of intercepted data by UK agencies, but do not deal with guidance on the *disclosure* of intercepted data in any detail.
[17] *Liberty's Submission to the Reviewer of Terrorism's Investigatory Powers Review*, November 2014.
[18] See http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata.

28. General Michael Hayden, former director of the NSA and the CIA, has publicly stated:

    We kill people based on metadata.[19]

29. Restrictions on the disclosure of metadata should therefore be no less stringent than restrictions on the disclosure of the contents of communications.

30. In summary, the framework governing the disclosure of intercepted data to foreign powers needs to be considered and updated. In the meantime, relevant internal (or 'below-the-waterline', to use the language of the IPT) guidance should be disclosed, as APPG Officers have sought. It is noted that, in the Consultation Document, the Home Office accepts in principle that there ought to be "*a robust statutory framework for the use of such intrusive investigative powers*" and "*a strong system of safeguards in place*". An analysis of the ISC report is beyond the scope of this Submission; however the APPG notes the conclusion of the report: there is a pressing need for new legislation.[20]

31. The Home Office is invited to give particular consideration to the ISC recommendation that the circumstances in which data may be shared, including constraints on intelligence sharing, should be set out clearly and comprehensively by statute[21].

32. As further noted in the ISC Report, there is also an issue as to the adequacy of safeguards on the sharing and disclosure of intelligence reports prepared by the UK agencies (as distinct from raw intercept data). The default position appears to be that all such information is sharable.[22] Again, this falls outside the scope of the current consultation, which is concerned with the interception of communications, although it is also a matter of concern to the APPG. To the extent that intelligence reports refer to identifiable individuals, they clearly interfere with the Article 8 rights of those individuals. For all the reasons outlined above, such interferences should be subject to strict safeguards. A default presumption that intelligence reports are 'sharable' would seem to be fundamentally incompatible with the UK's obligations under the ECHR.

33. It would be wise to consider different types of intercept and other data that may need different consideration in the statutory scheme; and the appointment of a person or team with responsibility to assess the risk that end-use of data may be unlawful.

'EXTERNAL' AND 'INTERNAL' COMMUNICATIONS

34. While the APPG's primary concern is with the sharing of intelligence data with foreign powers that carry out drone strikes, it also has an interest in the intermediary steps in the intelligence-gathering process leading up to the sharing of data.

35. The APPG therefore points out that there is a lack of clarity in the distinction drawn by RIPA between 'internal' and 'external' communications. The Code (as in previous drafts)

[19] Ibid.
[20] ISC Report, Annex A, para YY(g).
[21] At Zg
[22] ISC Report, para 243.

emphasises that communications are not 'internal' by virtue of the fact that they pass through the British Island *en route* to their destination (para 6.5). It gives the specific example of an email sent from a person in London to a person in Birmingham, routed via foreign IP addresses, which is an 'internal' communication.

36. This is clearly correct, and consistent with the legal advice that the APPG has already seen. However, in the *Liberty* IPT case, Mr. Charles Farr, Director General of the Office for Security and Counter Terrorism in the Home Office, gave evidence that web searches on Google, 'tweets' on Twitter and public messages on Facebook were considered to be external communications. Mr. Farr's view was that the recipients of e.g. a 'tweet' were not its readers but rather the Twitter web server. The APPG suggests that this is an overly technical interpretation of RIPA, not consistent with the approach to emails set out in the Code and not in the spirit of the legislation. The Code does not deal with this point.

37. In light of the increasing use of social media platforms as an alternative to conventional email, it would seem that treating social media messages as external communications could undermine the RIPA scheme, which gives greater protection to communications passing between people in the British Islands.

38. At the very least, the APPG suggests that the final draft of the Code set out expressly the Home Office's position on web searches, tweets, Facebook messages, etc. Once that is clear, there will be scope for further informed debate.

FURTHER ACTION

39. Given the use to which intercepted data may be put once shared with foreign powers – *i.e.* the facilitation of drone strikes – the APPG requests that the Home Office critically evaluate the existing (i) statutory framework, (ii) practice, (iii) non-statutory safeguards and (iv) oversight provisions relating to the intelligence-sharing of intercepted data, either in parallel with or immediately following this consultation exercise. This would naturally require input from other Government departments, but as the department responsible for the regulation of data intercepted in the UK, it is the place of the Home Office to initiate such a review. For all the reasons set out above, the APPG considers that review and oversight of UK-US data sharing arrangements have been neglected.

40. The APPG considers that, as a minimum, the following is necessary:

    a. In granting a warrant, consideration must be given by the Secretary of State to the ultimate use to which intercepted information is to be put. The risk that data is or may be used to facilitate lethal drone strikes must be relevant to the assessment of proportionality and considered not simply at the point at which data is to be shared with foreign powers, but at the time of its proposed interception. The Secretary of State must also be empowered to place appropriate constraints or conditions on the end-use of intercepted data at the time of granting a warrant. The same goes for the grant of authorisation for the interception of metadata pursuant to section 22 of RIPA. This should be set out in the Code.

    b. The sharing of intercepted (and other) intelligence with foreign powers must in each

case be subject to a formal, comprehensive framework – for example a bilateral agreement, annex to the 1946 agreement or a memorandum of understanding – setting out the uses to which data may be put, and those to which it may not be put.

41. The APPG hopes that the Home Office will also support its request to the Foreign and Commonwealth Office, made jointly with Professor Sir David Omand and Professor Michael Clarke, for disclosure of the Guidance that applies to the transfer of data available for use to target suspected terrorists outside traditional battlefields by the United States. Pending full review, and the implementation of proper statutory safeguards, disclosure of such 'Drones Guidance' is of critical importance and very much in the public interest.

42. The APPG further notes that the Obama administration in the US has engaged actively in high-level debate regarding the interception of data concerning US citizens, and is likely to be receptive to proposals for reform. In 2014 Timothy Edgar, who served under President Obama as the first director of privacy and civil liberties for the White House National Security Staff, engaged in debate with David Davis MP (and others) at an event held at Westminster. As Mr. Edgar subsequently put it in an email (disclosed with his permission):

    *The only publicly available version of the existing agreement [*the UKUSA Agreement*] was declassified in 2010 and is available on the NSA's website. It is very much out of date. It would be worth thinking about what a new agreement would look like and how it would incorporate protections for privacy and civil liberties. The drones issue is only one of the most dramatic issues that highlight the effect that intelligence information has.*

43. Finally, it would be worthwhile for the Home Office to consider critically the benefits of intercept data. The Consultation Document states that the Code is based on the premise that intercept material is a "*vital tool in the fight against terrorism and serious crime*". It asserts that "*since 2010, the majority of the MI5's top priority counter-terrorism investigations have used intercept capabilities in some form*". However, no in-depth analysis of the use and benefit of intercept material obtained through bulk collection appears to have been carried out. By contrast, a White House review group in the US has found that such data is not essential and could have been obtained by conventional means.[23] Detailed research by Peter Bergen at the New America Foundation has concluded that bulk phone records have had no discernible impact on preventing acts of terrorism.[24] The APPG invites the Home Office to commission comparable rigorous, independent research into the factual assertions that underpin the Code. This should in any event be done before a new Bill is drafted.

CONCLUSION

44. The APPG is concerned by the lack of statutory or other safeguards on the disclosure of intelligence data to foreign powers. In light of the IPT's judgment in the *Liberty* case it is highly likely that current arrangements – which give the executive a very wide discretion – are not ECHR-compliant. The lack of clarity in the law as it stands is particularly problematic in light of

[23] '*Liberty and Security in a Changing World*', December 2013, available at: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[24] 'Do *NSA's Bulk Surveillance Programmes Stop Terrorists?*', January 2013, available at: http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf

the lethal consequences of sharing data with foreign powers that use the data to carry out drone strikes against non-combatants. The implications of this demand careful review by the Home Office (as well as Foreign Office).

45. The APPG also takes the view that some of the intermediary steps leading up to the sharing of intelligence require clarification. The Code should state expressly whether the Home Office characterises web searches and messages on social media platforms as external communications. Moreover, the Code, and the legislative framework around it, should not assume that metadata is somehow more benign or less significant than the content of communications.

46. The APPG encourages the Home Office to implement rules that (i) compel the Home Secretary to consider the end-use of intelligence data at the stage of granting a warrant and (ii) limit the circumstances in which certain types of data may be disclosed to a foreign partner absent understanding and agreement as to the ultimate use. At the least, the Code should address the need to take end-use by a foreign partner into account.

47. More generally, the APPG suggests that more work needs to be done to investigate the benefits of bulk interception, given the significant level of interference with individual rights that it necessarily entails.

48. This Submission is not an official publication and may not represent the views of individual APPG members.

This submission is made by the following named officers, on behalf of the All Party Parliamentary Group on drones:

Chair: Tom Watson MP (Lab);
Vice Chairs: Baroness Stern (CB); David Davis (Con); Treasurer: John Hemming MP (LD);
Secretary: David Anderson MP (Lab).

For any further information, please contact the APPG's Researcher Anna Thomas on anna.thomas@parliament.uk

March 2015

Association of Chief Police Officers

Report of Richard Berry, National Policing Lead for Communications Data

Responses to Questions tabled by David Anderson QC

Dear Sir,

As Chair of the National Policing Data Communications Group, my role permits me to communicate views of colleagues, who acquire communications data on a daily basis as part of their role as Single Points of Contact within law enforcement and perhaps more generally than the specific organisations from which you will also receive evidence.

Communications data (CD) provides vital support to policing in particular, in delivering against our objectives in relation to public safety, proactive and reactive investigation of crime, both specialist in nature (such as counter-terrorism and child sexual exploitation) and in relation to a spectrum of criminal investigations including, murder, kidnap for ransom, other offences involving the use or threat of violence, armed robbery, people- and drug-trafficking as well as less serious offences.

In respect of all of these investigation types, CD enables police to establish a chronology of events; associations between individuals whether victims, witnesses or perpetrators; can assist in confirming or dispelling suspicion, based on the location of individuals at the time that specific communications were transmitted or received; and, can provide vital corroboration of other intelligence or evidence, which may be probative in value or have the effect of assisting in the identification or recovery of other evidence.

Crucially, the way communications technology has evolved in the last decade, particularly among younger people, has put unique pressures on police investigating reports of vulnerable missing people. Many of these are youngsters, whose primary means of communication is what have become known as Over-the-Top (OTT) services (more commonly, for the most part, referred to as ‘Apps’). The use of these is not generally visible to the communications service provider (CSP) or subject of mandatory data retention. Additionally, the providers of many of these services are situated in other jurisdictions, often in time-zones which render contact more difficult that would normally be expected, and where difficulties of language, culture and understanding of potential legal processes

involved can lead to the frustration of investigations where the safety of vulnerable young people is a paramount concern.

Forthcoming changes to CSP infrastructure, as Internet Multimedia Subsystems (IMS) is rolled out, are likely to exacerbate this growing problem and providing the additional complication, through delivery of 'seamless interoperability', of data fragmentation and the resultant requirement to ask the same question of a number of CSPs, who may be simultaneously involved in the provision of any given communications event.

In answering the questions posed in your letter of 1st August, I have examined the extent to which material provided in relation to the consideration of the draft Communications Data Bill in 2012 is still current and may assist and, where it is appropriate to do so, I will include that material in answers to your questions.

Question 1 - What are the threats and risks with which you are dealing?

Many of the requirements placed upon law enforcement and policing in particular relate to what may be described as public safety activities – whether these relate to the public in general, a section of the public or to an individual, and in general terms these relate to the assessment or perception of risk, whether to individuals or to society at large. A significant proportion of operational activity relates to young, or otherwise vulnerable, missing persons. Due to the fact that this group in particular do not necessarily communicate by 'traditional' means, their communications methods have to be identified by investigators and where such communications are identified, typically an internet application will be the relevant medium (e.g. Whatsapp) and the providers of such services are not based in the UK and there is no ready mechanism lawfully to acquire relevant information in an expedient fashion. This in itself is a problem for which police have no ready solution.

Crimes in action, (which include for example kidnap for ransom, false imprisonment, food contamination and other kinds of blackmail) provide similar, unique challenges to law enforcement: in all such cases, some form of life-threat is implicit and the requirement to obtain communications data to assist the investigation is urgent and may be impeded by jurisdictional and time-zone issues.

Trafficking offences whether relating to people, drugs or weapons will typically follow patterns where those involved have been engaged over often significant periods of time before offences come to light. The requirement to obtain communications data may reach back in point of time to the oldest data potentially available to investigators: this is necessary to identify participants, their specific role in the offences under investigation and for the probative value of the data – not least in demonstrating association and common purpose – as required for all conspiracy or joint enterprise offences.

Communications data is often critical in the investigation of crimes of violence such as murder, serious and other assaults including domestic violence. Sometimes these investigations are resolved when some time has passed, loyalties have changed and persons come forward with hitherto unknown information, where CD can provide vital corroboration. This is particularly so, where corroboration is sought for criminal or vulnerable witnesses.

In relation to online Child Sexual Exploitation, CEOP will doubtless be able to provide significant submissions; but the physical abuse of young people is often orchestrated and whether 'grooming' takes place online or not, CD is vital in providing investigative leads and ultimately in providing the evidence required to secure conviction.

A significant proportion of investigation activity is devoted to fraud and financial crime more frequently carried out over the internet: this figure does not include data from specialist cybercrime units but is part of the growing threat of cybercrime. Other specific online offences include harassment and malicious communications, accounting for nearly 7% of lawful data acquisition. These figures tend to suggest that cybercrime is not solely the responsibility of specialist units, but is a growing general policing challenge.

Other serious and serial offending - The results of the 2012 SPoC survey contains a breakdown of other offences where communications data is used to address threats and risks to individuals and the public.

From time to time, there is a requirement from the High Court in order to assist in the protection of children who are Wards of Court and perceived as being at risk; police may also

be asked to assist where there is a requirement from defence teams to assist with CD which may be beneficial to preparation of a defence case.

CD can also be helpful where it is acquired to determine whether or not an individual can be eliminated from further enquiries, including where lawfully acquired CD may support an assertion of alibi.

A full statistical breakdown of these activities is included within the answer to Question 2 below.

Question 2 - 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.

These comments relate only to the use of Communications Data;

CD is helpful in corroboration of witnesses and assisting in the identification of suspects and witnesses. CD of any kind is only ever corroborative of other evidence in a case, but may provide vital support for any or all of the following:

A. Chronology – most communications events are capable of having a specific time attached to them – it may be necessary to consider the implications of device time against network time or time zone applicable to a particular transaction or series of transactions. It may also be necessary to consider the accuracy of any temporal information received;

B. Association and common purpose – the former will normally be self-evident and the latter may be inferred from other known facts;

C. Presence or otherwise at a geographical locus – the range and nature of devices which can connect to mobile, fixed and wireless networks mean that particular care must be taken to maximise the potential evidential benefit associated with location information by properly attributing device or application usage (see below);

D. Corroboration of vulnerable or criminal witnesses.

Communications Data may also provide corroborative evidence relating to the attribution of user accounts and devices to individuals.

Reproduced below are the statistics obtained from the SPoC Data Survey that was conducted in 2012 and prepared in relation to the draft Communications Data Bill.

In June 2012 the ACPO Data Communications Group conducted a two week survey within SPoC units across UK law enforcement agencies. This survey looked at the acquisition of communications data and provides the reader with an insight into the usage of such data across UK law enforcement. The survey results provide a very short snapshot of how communications data is used across law enforcement agencies. This data only relates to the acquisition of communications data under Chapter1 Part2 Regulation of Investigatory Powers Act 2000. This survey was undertaken by 62 UK law enforcement agencies.

The survey took place between the 4th June and 17th June 2012 and requested details to be recorded that covered the following categories:

- Crime type under which the communications data was being requested
- Type of communications data being sought
- Age of communications data
- Grading of data requests
- Data subject identification
- Request identifier types

This survey was undertaken at the point when an application is submitted by the applicant to a SPoC. A SPoC is the Single Point of Contact who is an accredited individual responsible for acquiring the data from communication service provider.
This report will only provide the reader with percentages in relation to the acquisition of communications data. No numbers will be provided due to the interests of national security. ACPO Data Communication Group also provided a commitment to all those who took part in the survey to the fact that the actual numbers relating to the survey will not be published.

Full list of offences listed in descending order

Offences	Percentage
Drug Trafficking	17.7%
Drugs Misc	6.9%
Homicide (Any)	6.7%
Burglary (Res & Non)	6.5%
Fraud	6.5%
Missing/vulnerable	5.7%
Firearms	5.2%
Other	4.3%
Harassment& Stalking	3.4%
Malicious Comms	3.2%
Theft	3.0%
Serious Assault	2.9%
Child Abuse	2.9%
Other sexual	2.7%
Armed Robbery	2.7%
Rape	2.4%
Street Robbery	1.6%
Robbery	1.4%
Attempt murder	1.1%
HMRC offences	1.1%
Kidnap	1.1%
Terrorism	1.1%
Theft of/from MV	0.8%
Money Laundering	0.7%
Bribery & Corruption	0.7%
Blackmail	0.5%
People Trafficking	0.5%
999	0.5%
E-crime	0.5%
Immigration	0.4%

Criminal Damage	0.4%
Bail & Courts	0.4%
Conspiracy	0.4%
Agg Burglary	0.4%
Arson	0.3%
Forgery Counterfeit	0.3%
Minor Assault	0.3%
Sexual offences	0.3%
Racial Hatred	0.3%
Threats to kill	0.3%
Gang related	0.3%
Public Order	0.3%
Sexual Other	0.2%
Bomb Hoax	0.1%
Obscene Pubs	0.1%
Sex Industry	0.1%
False Impt	0.1%
Vehicle crime	0.1%
Death by	0.1%
Domestic abuse	0.1%
Explosives	0.1%
Witness Intimidation	0.1%

Chart 1:

Chart 1 shows percentages in relation to the crime type that a communications data request was made during the survey period.

The following charts provide further information in relation to specific areas of Crime Types, Time Periods (Age of Data) RIPA Request Types, Data Subjects and National Request Prioritisation Grades:

Crime Type

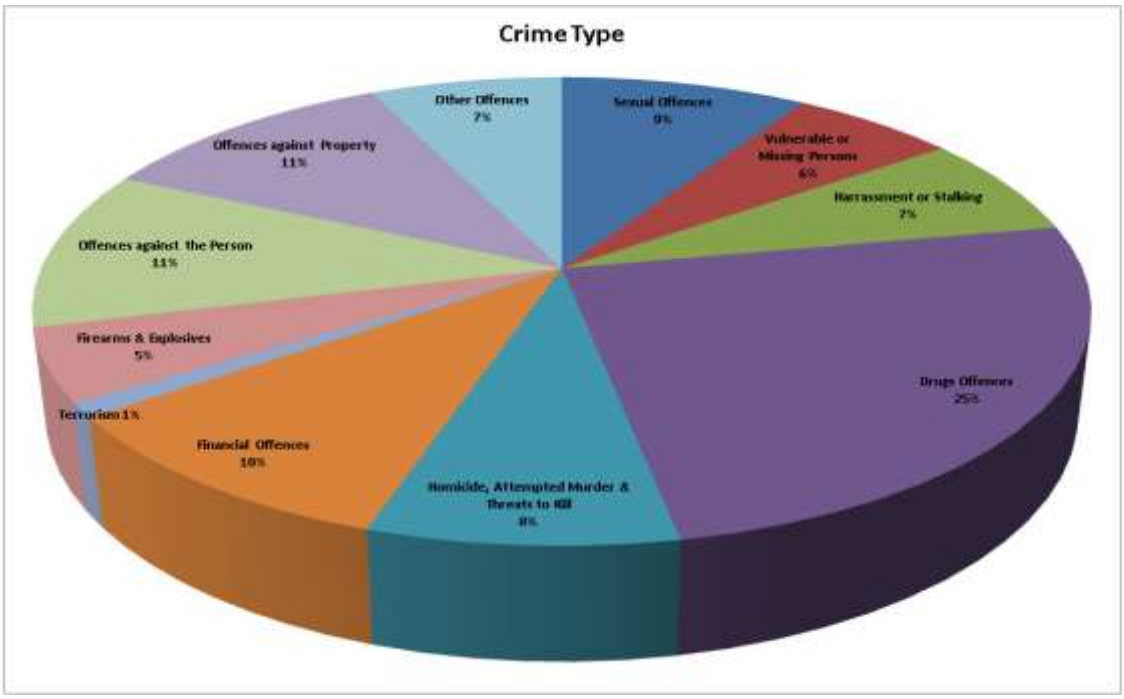

Chart 2: Breakdown of Enquiries by Crime Type

The above chart shows the relative proportions of different crime types for which communications data was requested.

- 25% of communications data requests related to drugs investigations.
- 9% of communications data requests related to sexual offences investigations.
- 6% of communications data requests related to missing/vulnerable persons investigations.
- 8% of communications data requests related to homicide, attempt murder and threats to kill investigations.
- 11% of communications data requests related to property offences, burglary and theft investigations.
- 7% of communications data requests related to harassment and stalking investigations.
- 5% of communications data requests related to firearms and explosives investigations.
- 10% of communications data requests related to financial offences, fraud and money laundering investigations.
- 11% of communications data requests related to offences against the person, robbery, assault, kidnap investigations.

- 7% of other communications data requests related to gangs, arson, bomb hoax and immigration investigations.
- 1% of communication data requests related to terrorism investigations.

Time Periods

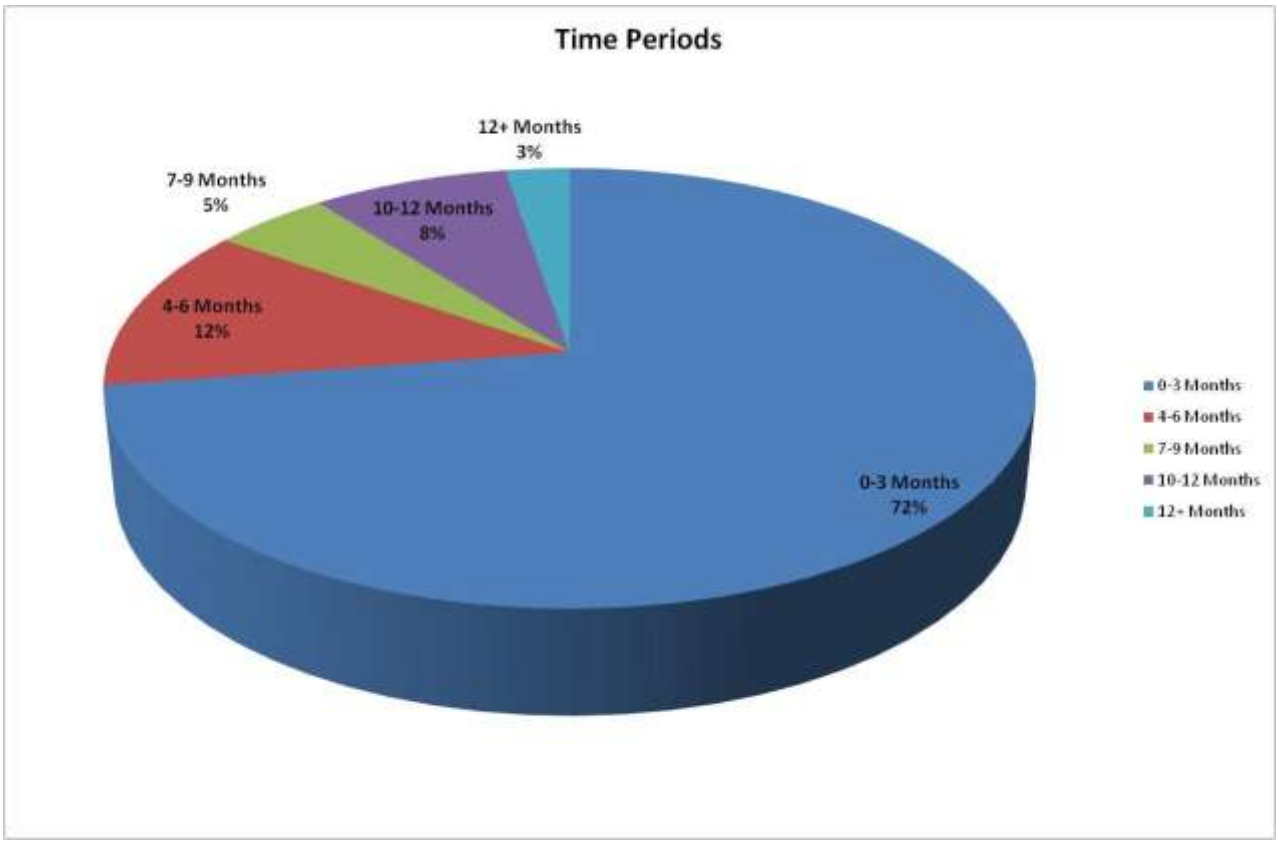

Chart 3: Breakdown of all Enquiries by Time Period

The above chart shows how long communication service providers have held the relevant data that was requested during the survey.

84% of communications data requested was up to 6 months old.

13% of communications data requested was 7 – 12 months old.
What should be recognised is that 10-12 months data accounts for 8% this is higher than the 7-9 months data request as investigators realise that they risk losing this data as under the EUDRD, CSPs are not obliged to retain data beyond 12 months.

3% of communications data was more than 12 months old. Although this data does not need to be retained under the EUDRD, this data is retained by some communication service providers for their own business purposes.

RIPA Request Types

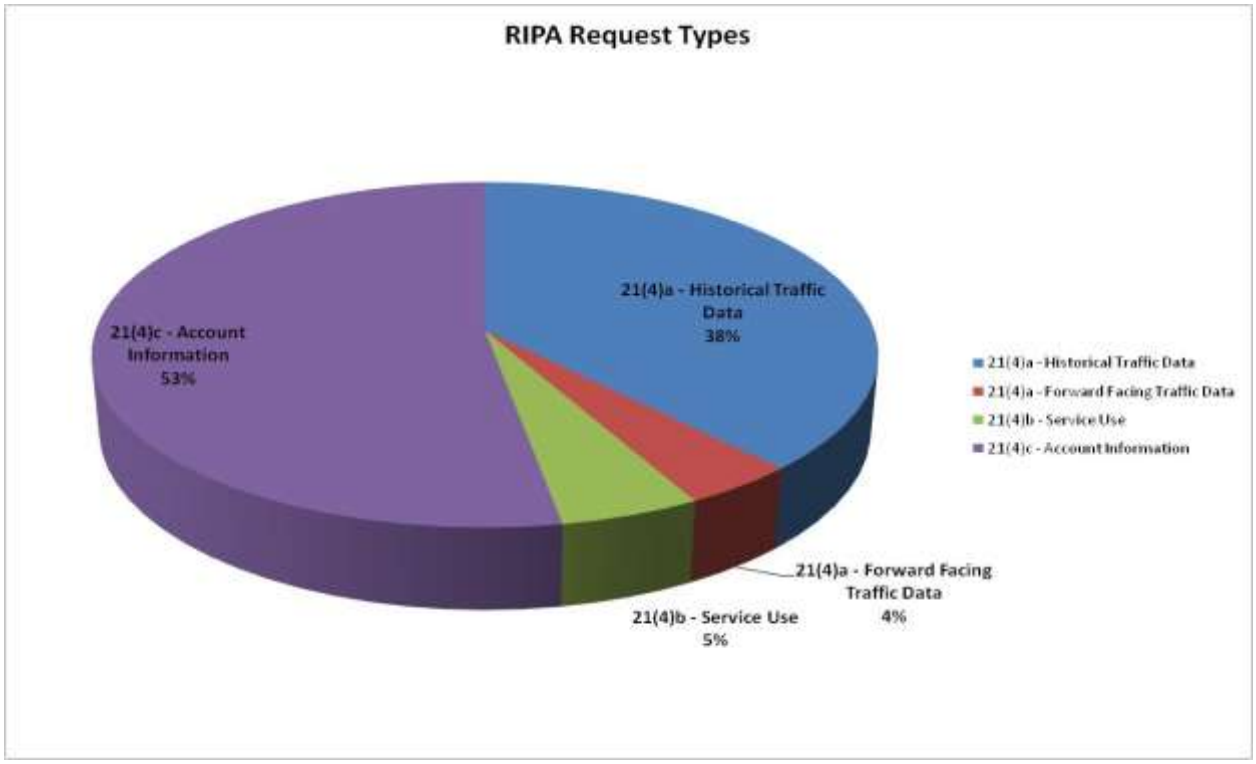

Chart 4: Breakdown of all enquiries by Request Type

Section 24 (1) of RIPA, in this Chapter "communications data" means any of the following:

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;
(Historic data requests relate to a date period in the past, whilst Forward Facing data requests relate to dates in the future)

(b) Any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—
(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

Data Subjects

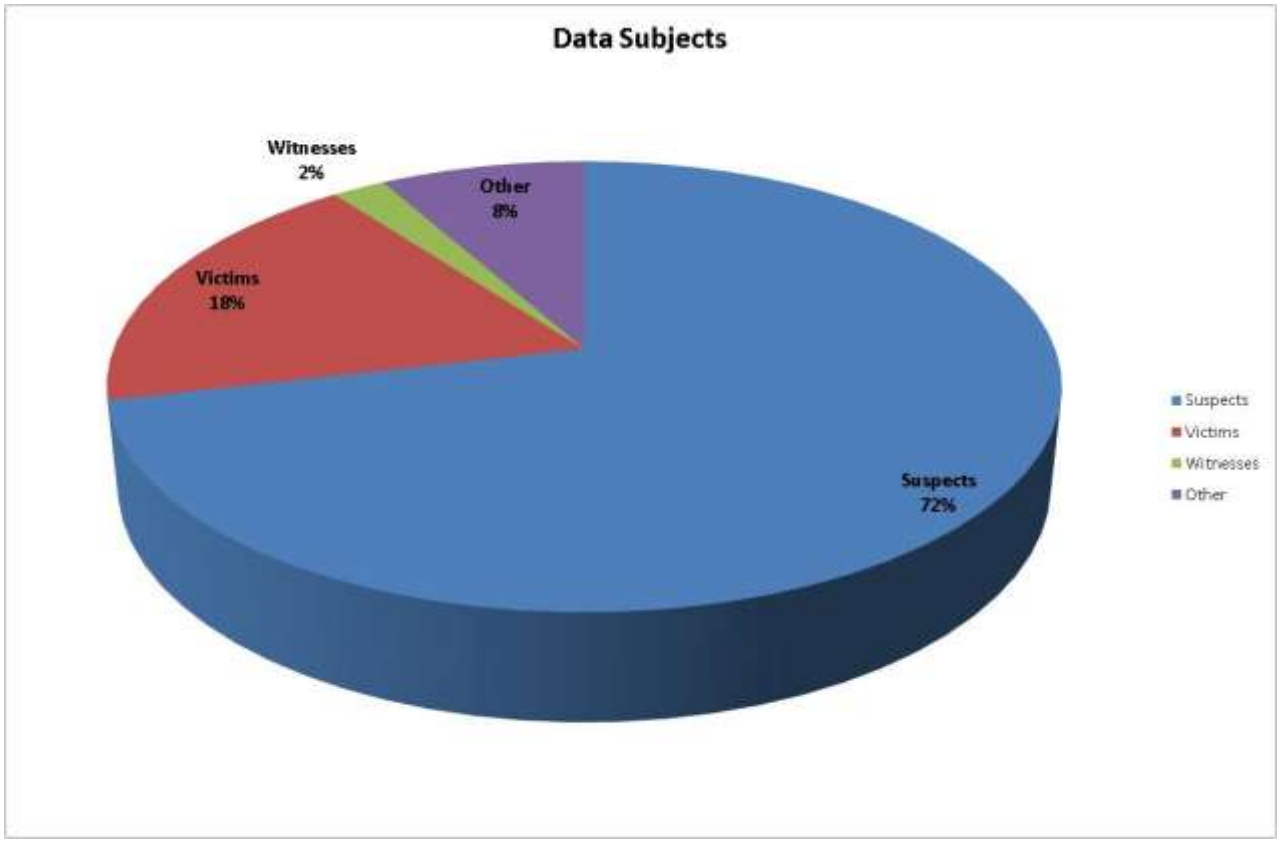

Chart 5: Breakdown of all enquiries by Data Subject types

The above chart identifies the person who the communications data request related to.
72% of the communications data requests related to suspect enquiries; this would clearly be in relation to the prevention and detection of crime. (A suspect is a person who has been arrested charged or believed to be responsible for a criminal offence at a particular time)
18% of the communications data requests related to victims of crime, this could be because their electronic device had been stolen or that communication data was used during the commission of a crime.

2% of the communications data requests related to witnesses, this could be identifying the actual time of a call, identification of a witness through possession of their telephone number. 8% of the communications data requests related to other which could relate to missing persons and vulnerable individuals, persons of interest during a homicide investigation or persons whose status at the time of the submission were unknown.

Whilst this report captures the number of data subjects listed within each application, it is important to remember that multiple applications are often submitted for a single investigation. In this survey 44 investigations accounted for 10 or more RIPA requests. There was one investigation in which over 40 RIPA requests were made.

Grades

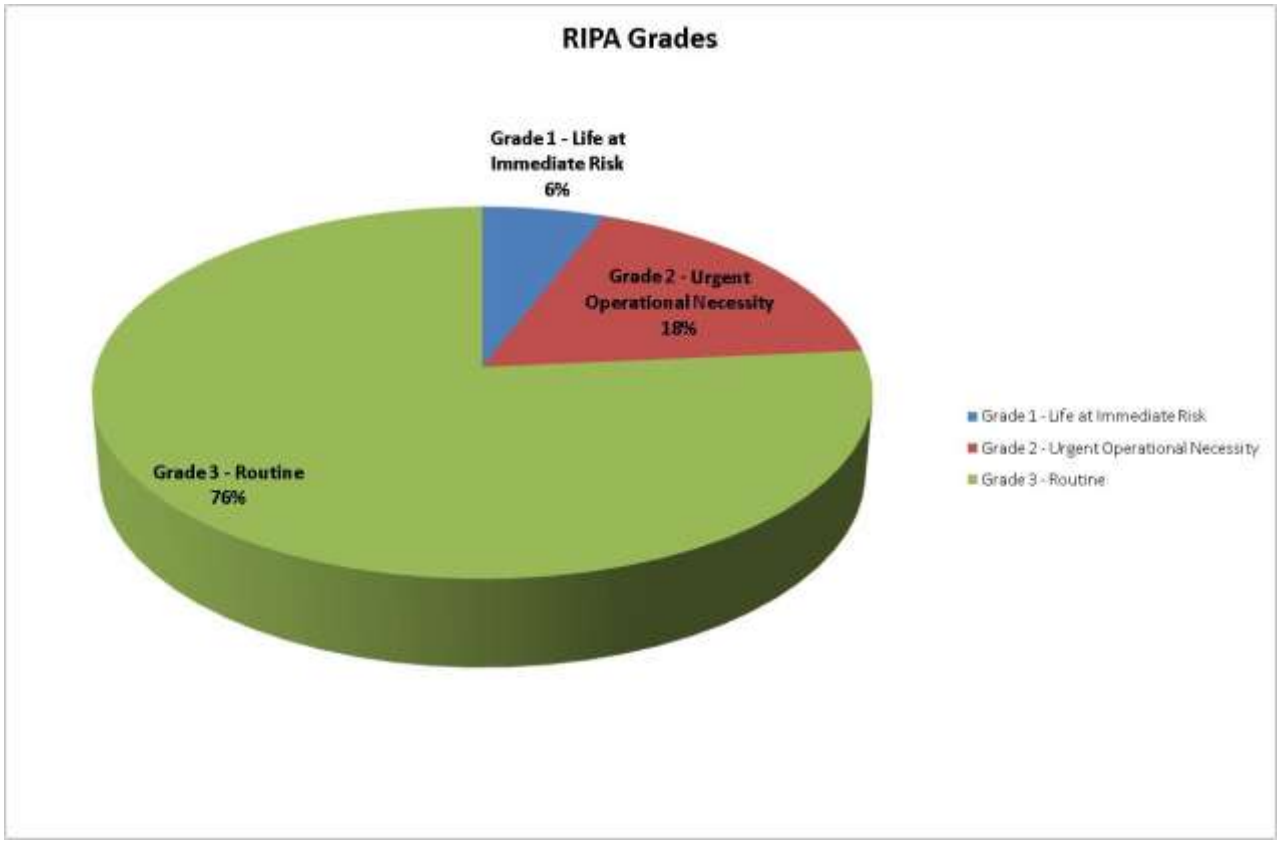

Chart 6: Breakdown of all enquiries by RIPA Grade

The above chart sets out the grade of the communications data request made by law enforcement to the communication service provider.

The Data Communications Group (DCG) which comprises representatives of CSPs, UK law enforcement and other public authorities to manage the strategic relationship between public authorities and the communications industry has adopted a grading scheme to indicate the

appropriate timeliness of the response to requirements for disclosure of communications data. There are three grades:

• Grade 1 – an immediate threat to life;

• Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security;

• Grade 3 – other enquiries that are less time critical but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime

The emphasis within Grade 1 and 2 is the urgent provision of the communications data will have an immediate and positive impact on the investigation or operation.

Significant Findings

It was evident from the survey that law enforcement is not able to define serious crime. Most definitions that are used are very subjective and what may be classed as serious to one victim may not be serious to another.
The same can be said in relation to other less serious crimes, it is for this reason that we have not included percentages around these areas.

Crime Types

- 25% Drugs Investigations
- 7% Homicide Investigations
- 6% Missing Person and Vulnerable Person Investigations
- 21% Theft Act and Offences Against the Person Investigations

Data requested from communication service providers

- 95% Related to account information or traffic data
- 72% Requests were suspect related
- 20% Requests were victim or witness related
- 24% Requests were due to life at risk or urgent operational necessity

Older data is clearly used less, but data older than 6 months still accounts for a significant number of requests.

- 37% Of data requests relating to sexual offences was older than 6 months
- 27% Of data requests relating to Terrorism was older than 6 months
- 11% Of data requests relating to Drugs was older than 6 months
- 5% Of data requests relating to Homicide/Attempt Murder was older than 6 months
- 9% Of data requests relating to Firearms and Explosives was older than 6 months

Although this survey is only a snap shot over a two week period, this data does provide us with an insight into how, why and for what purpose communication data is used.

It is clear that communications data is paramount in enabling law enforcement agencies to protect the vulnerable and saves lives.

The increase in communication over the past decade and the increase predicted for the future make it even more important for law enforcement to be able to use the least intrusive investigative technique to prevent and detect crime today and in the future.

The acquisition of communications data is one of the least intrusive investigative techniques undertaken by law enforcement and is a process that is strictly managed and authorised by senior police officers in accordance with RIPA Chapter 1 Part 2.

The process ensures that the designated person complies with the requirements as set out in Chapter 1 Part 2 RIPA giving due consideration to a number of factors;

- Likely engagements of Human Rights,
- the necessity of the request,
- the purpose must be for the protection of vulnerable persons or for the purpose of

preventing or detecting crime,

- the authorising officer must be satisfied that it is necessary to use communications data in the investigation,
- The proportionality; consideration will be given to balancing the seriousness of the crime being investigated and the interference with the privacy of the individual concerned.

The internal processes implemented and the national governance and inspection regime by IOCCO ensures that this investigative technique is only used in the protection of vulnerable persons and the prevention and detection of crime.

The need for law enforcement to maintain and improve on this capability is fundamental in our ability to keep pace with new technology, protect the vulnerable and continue to prevent and detect crime.

Question 3 - 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?

Dealing with threats and risks faced over the last couple of decades has been characterised by understanding two things: how consumers (and therefore subjects of an enquiry) use communications technology; and, understanding enough about the CSP business model, products and particularly data derived from the use of those products, which can assist investigations. Legislation regarding the means of lawful CD acquisition and mandatory retention of the data most useful to investigators has together with specialism developed in SPoC units. Historically this has created adequate means to cope with operational challenges, however, as the communications market has evolved and influenced consumer behaviour; SPoCs are increasingly facing difficulty in fulfilling their role. In part this has been and is being mitigated by attention to training and tradecraft, to ensure that there is adequate understanding of opportunities, risks and challenges posed by newer technologies. This work must attract sufficient funding to continue delivering benefit throughout the country.

The prevalence of Over the Top (OTT) services referred to in the introductory note above means that more ‘traditional’ CSPs are blind to the traffic they are carrying across the

network. There are a number of ways of addressing this but clearly alternative investigative methods have to be considered, whether these are network-based or forensic in nature. We would welcome the opportunity to discuss both of these alternatives in more detail than may be suitable for a document of this nature.

A significant challenge to our future capabilities is in relation to IP Multimedia Subsystem. The mobile CSPs are undertaking a step-change to how they provide voice services by phasing in the provision of voice over data connections through the introduction of IP Multimedia Subsystem (IMS) frameworks, the first deployed applications being VoWifi and VoLTE. This change will have a fundamental impact on the availability and usage of CD for traditional voice and SMS services. For example:

- CSPs may not capture and retain similar types of CD for IMS related calls/SMS as they do for traditional services;
- Voice/SMS CD will become fragmented (depending on how the call is provisioned) with the various fragments containing different information (e.g. some CD will no longer have Geo data, or will have it in a different format).
- Attribution may become more difficult as voice/SMS communications become disconnected from the SIM and device provided by the CSP.
- Analysts receiving the CD from affected CSPs will need to understand the meaning of the new fields that IMS brings, and be able to piece together the fragmented CD.
- Future Rich Communications Services (RCS) will introduce further complexities and the resulting CD will have aspects of both voice and data.

I would like to expand upon IMS and offer some wider thoughts on the future of CD, digital intelligence and investigations. It is my observation that some parties who seek to engage in the communications data social/legal debates, do so from a limited aperture upon the extent of social and economic changes we will see in coming years. Technology, as a strategic driver for change, brings new complexity and risks that law enforcement must now position itself to address in the near future. The Chancellor has previously signalled the intention of Britain being recognised as a safe place to conduct business online. The threats surrounding cybercrime playing out in the digital and real worlds is rapidly becoming a national interest. Here are a number of CD related issues we are considering:

• Cloud based services expand and become the norm in some sectors of the economy. Law enforcement is driven by forensic regulation. Will CD data be accessed through a cloud forensic process or simply obtained as CD? With data packets being the vehicles of communication my industry colleagues are faced with the dilemma of such forensication possibly being considered as content and therefore potentially intercept material. We then have the added complexity that such communication may be based in or routed through server networks outside of the UK.

• Private and public bodies are maturing their approaches to bulk analytics and 'big data'. This will involve what is often referred to as 'machine learning' and artificial intelligence. We have been engaging with academics and mathematicians working is this area. There is much work underway developing algorithms to understand risk and threats in society and CD will be a major feed into such work as law enforcement will arguably need to draw new inferences from aggregated datasets. Anticipating this and the need to foster public confidence and trust we have been working with the College of Policing looking at developing ethical practice to supplement the legal framework that we use in CD and digital investigation. Industry has no ethical framework within which it operates. This has resulted in self-generated transparency reporting such as that published by Vodaphone in 2014.

• The Internet of Things will increasingly become reality with a proliferation of non-human use of IP addresses. Recent estimates suggest that the sheer numbers of devices in existence by 2020 could be creating literally fields of 'IP haystacks'. Recent investigations have shown that malware can redirect routers *en masse* to child abuse imagery. In one operation over half a million routers were directed at this material in very short periods of time. Bulk analysis of IP data may become an operational necessity in some cases.

• There are many commercial interests in digital and cyber investigation. They operate outside of legislation such as RIPA. Some have capabilities which law enforcement may never have and therefore, any future legislation may need to be cognisant of this trend. Cyber security companies are legitimate partners for law enforcement when trying to work through highly complex and fast moving cyber enabled crime.

Risks

- More difficult to attribute a device to a person.
- More difficult to discover the true user of a identifier.
- More difficult to identify the location of the device at the time of use or when trying to locate

a victim.

- More difficult to identify which service has recorded some of the data, resulting in fragmented data.
- More difficult to separate CD and intercept material
- More difficult to analyse without bulk machine-based techniques.
- Significant increase in training staff to understand difficulties associated with IMS and a concurrent need to train more staff in Radio Frequency Propagation Surveys in order to survey every investigation to identify potential service carriers.

Encryption

It is unclear at this stage to quantify what the increased use of encryption will have upon our ability to obtain data, or the extent to which this will impede work in the communications data environment; but, it is clear that some difficulty is likely to be encountered in separating traditional CD (or internet meta-data) from what has been traditionally regarded as 'content'. The increasing prevalence of encryption technologies in consumer facing hardware, software and services has the potential to greatly increase the technical sophistication and capacity required by law enforcement to access material protected in such a way. It may be too early, at this stage, to comment definitively: those better informed technically may be able to address this point in more detail.

Question 4 - 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?

In addition to the use of Communications Data, legislation has provided law enforcement with a raft of investigative options when undertaking an investigation, some that are more intrusive than Communications Data, others that we would say is less intrusive, some that is more expensive to undertake, others that is less expensive. What we can say is that a number of crimes that are committed can only be investigated by obtaining Communications Data. So although we provide options around alternatives, each investigation is undertaken taking into account the justification in what actions we are undertaking, the necessity of our actions and the proportionality of our actions against the offence being investigated.

- In proactive investigation, where CD is utilised, this will have the effect of providing a less intrusive means of surveillance.
- There is a much greater interference with the privacy of individuals when using for example: conventional surveillance; any of a number of forms of technical surveillance;
- The alternatives to the use of CD, whilst more intrusive, tend to have higher associated cost (in equipment and workforce deployment); higher risk (whether to surveillance teams or individuals employed); and, they are more workforce intensive, whether for actual teams physically deployed, or for personnel monitoring technical equipment – this involves having a highly-skilled workforce available, with attendant cost.
- While law enforcement agencies are finding themselves cash-strapped, it is difficult to envisage how chief officers could employ and equip a workforce capable of undertaking these activities, all of which have significantly higher cost than the use of CD.
- Alternative means of proactive investigation are used sparingly and with full justification. In the absence of an ability to use CD effectively, there is a likelihood that a greater volume of more intrusive law enforcement activity could result in some form of lowering the threshold for the authorisation of such activities and the greater use of such techniques undermining public confidence in law enforcement.
- Open Source research on the internet (searching material which is publicly available) would provide some benefit, both to proactive and reactive investigation, but is not perceived as being a realistic alternative to the range of activities considered in the foregoing.
- With the exceptions of Open Source research and digital forensics (by which is meant the downloading in whole or in part of electronic equipment seized by police, in accordance with lawful authority), none of the techniques described lend themselves readily to reactive investigation – which, of course, includes any of the trafficking offences, murder and child sexual exploitation.
- The inevitable knock-on effect of the foregoing is growing police inability to carry out primary operational activity, particularly in the field of public safety operations (for example, vulnerable missing persons or suicide interventions), with the concurrent risk of loss of public confidence for two reasons: (a) the growing number of investigations incapable of being progressed (e.g. into Child Sexual Exploitation); and (b) the possibility of a growing public sense of living in a 'surveillance state'.

Question 5 - 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 and the period of time for which the information should be available before the request to examine it.

In relation to future needs, this is clearly a very difficult and complicated area to address. When the 2000 RIPA Act was enacted who would have foreseen that we would be able to communicate with a person in another country via the internet i.e. VOIP; who would have foreseen that social media and the use of apps would be the norm in societies daily communication practices.
It is therefore against this backdrop that we face our biggest challenge in how do we ensure that whatever legislation is enacted keeps pace with technology and is future proof for many years to come.

I would suggest that our starting point to this lies within what our initial requirements were. The RIPA 2000 Act makes it quite clear that we are seeking access to data that identifies the Who, What, Where, When the How a communication took place. We would say that these are the basic requirements that we are seeking in relation to any communication that takes place in the United Kingdom. We do not believe that how this is undertaken or by whom this is undertaken is our concern, our concern is in relation to the fact that we need this data retained in order that we can gain access to the data in accordance with legislation.

We would suggest that unless this takes place in the future our ability to protect lives and investigate crime will be greatly hindered. Our stance has always been to the effect that this data should be retained for a minimum of 12 months, this is what we supported in the recent DRIPA Bill and we would suggest that the SPoC survey supports this requirement.

The value of CD in an investigation is dependent on the ability to determine the device and where appropriate, internet access information and use of any application (and through additional enquiry, the device or account user) used to originate a communication, the device(s) and recipient(s) of that communication; the equipment (for internet usage, the recipient access information, application and user identifier). The related identifiers might be **Account Information** held by the provider of the service, **Telephone Number**, **IP**

address, Application User ID, Equipment Identifier (e.g. IMEI, MAC) or other Service Identifier.

A **Date** and **Timestamp** (together with the **Time zone**) for records sought to be acquired, together with any information captured by the service provider in relation to the use of the device and its **Location** at a given point in time: in essence these items give investigators answers to questions which begin with **who, what, when, where.**

The statistical breakdown relating to requests for this information originating from the SPoC community appears above in the answer to Q2. However, it should not be assumed that all the required information is captured and retained, or even that when such data is retained that law enforcement will obtain lawful access to the information.

A broadly similar SPoC survey was carried out in 2005 (details can be supplied on request). The total number of requests for CD from the SPoC community then was not very different to the total number of acquisitions in 2012, a rise of roughly 10%. What has changed is the means by which the public communicate and therefore, the subsection of that public who attract the attention of law enforcement: in essence, therefore, the questions remain the same and the number of questions asked does not differ greatly – what is different is the growing number of questions which are asked of a wider range of service providers.

It follows that while the technology used by subjects of enquiry is changing and the nature of the questions is not, *any new legislation in this area should be worded in terms that are technology-neutral*.

Age of data requested: The SPoC survey (at page 8 above) deals with the period of time between the communication event and the request by law enforcement for access to related data. In essence, 72% of communications data requested was up to 6 months old. The figure rose to 84% at 6 months and 97% at 12 months. 3% of requests were for data over 12 months old.

13% of communications data requested was 7 – 12 months old.

What should be recognised is that 10-12 months data accounts for 8% this is higher than the 7-9 months data request as investigators realise that they risk losing this data as under the EUDRD, CSPs are not obliged to retain data beyond 12 months.

3% of communications data was more than 12 months old. Although this data does not need to be retained under the EUDRD, this data is retained by some communication service providers for their own business purposes.

The following paragraphs form an abstract from written evidence submitted to the Joint Committee in 2012 and relate to a number of specific **problems currently faced** by law enforcement in relation to CD:

National Policing Data Communications Group conducted a poll of Law Enforcement Agencies nationwide in an effort to establish whether the perception of the threats and risks in law enforcement capability is palpable.

That poll yielded significant examples which indicate that there are several significant threats around our ability to obtain communications data in operational policing – the widely-held perception being that the loss in our capabilities is growing.

The threats and risks are characterised in the following:

- Data which belongs to companies based out of the UK jurisdiction
- Data for which there is no business need and which falls outside the categories currently required to be retained.

The evolving nature of the manner in which people communicate has created, simply by consumer migration, a very real problem for policing. The recent Communications Market Report from Ofcom puts some meaningful context to this concept, (http://consumers.ofcom.org.uk/2012/07/uk-is-now-texting-more-than-talking/); showing that more than three quarters of the population use the internet, more than three quarters of UK homes have a broadband connection.

There are four mobile phone subscriptions for every three people in the UK and almost four in ten of those are internet-capable. Amongst younger people, text-based communication (not just text messaging) is a daily occurrence for most and data consumed has more than doubled in an eighteen month period, with two thirds of internet users having accessed Facebook.

The inescapable fact is that communications technology is changing the way people communicate, not just criminals, but the whole of the population. Many popular web-based communications applications – whether webmail or social networks – are based offshore; with many of the most popular being based in the United States of America. The data created by the use of these applications is not 'generated or processed' in the United Kingdom and is therefore not currently required to be retained by UK Communications Service Providers under either EU or UK law.

The fact that the Internet Service Providers who provide the internet access for users of these applications merely provide a conduit for access to and use of these services, under current legislation, means that the metadata (the data about the use of those communications applications), is not retained.

This is one element of the threats and risks.

That, however, is only a part of the problem. Many service providers are unable to resolve Internet Protocol (IP) addresses to end-user devices. The service providers have no business need to do so: many have tariffs which offer 'unlimited data' or charge for data consumption by volume. ISPs are in constant competition with one another, with factors such as price, coverage and speed of connection or bandwidth being key to the attraction of subscribers. It has been widely publicised that the current internet addressing system (IPv4) has run out of addresses for allocation. Expense and complexity mean that this situation will continue to prevail for some years. For several years, many ISPs have been assigning IP addresses dynamically, which typically means that a consumer will use a particular IP address only for one session, then it will quickly be allocated to another user. This creates practical difficulties with which investigators are very familiar, but is far from being an insoluble problem.

Of greater significance is the fact that ISPs increasingly have sought to overcome the issue of the IP address shortfall by the deployment of Carrier Grade Network Address Translation (sometimes expressed as NAT or CGN). This is a large-scale variant of the arrangement most commonly found in the domestic environment.

In some cases, for example, on a wi-fi network, this problem is exacerbated by the fact that the only identifying feature (identifier) of the device might be its Media Access Control (MAC) number. Unlike mobile handsets, SIM cards or other internet-capable devices, there is no universal numbering system for MAC addresses (devices which are capable of accessing the internet in more than one way, e.g. a typical laptop, may have more than one MAC number in any case). In most cases, where the device subject of the investigation is made available for examination, the MAC number question is readily resolved.

Finally, it is probably worth noting that in some states within the US, it is common practice that the CSP inform the subject of a law enforcement request for data within a set period. Many of our operations are covert in nature, often so that police involvement in a crime in action or an on-going investigation is not overt; or where there is an issue of exposing police methodology, or the extent of police capability. The fact that some providers will inform the subject does at time prevent requests being made and therefore prolonging some operations.

Question 6 - 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 information you are examining?

Legislation mandating the retention of CD by CSPs is necessary – the more so due to the fact that CSPs (who were reluctant to act to retain certain types of data in excess of their business requirement under the voluntary provisions of the Anti-Terrorism Crime and Security Act 2001) anticipate adverse consumer reaction to any perception of voluntary assistance to government, particularly due to the perception of the effect of the Snowden revelations on consumer choice. The retention regime should take account of necessity and proportionality, both in choice of CSPs to whom mandated retention should apply and the individual products (and data fields within products) subject of that requirement. Such a

regime minimizes the burdens on industry collectively and provides the greatest degree of coverage in relation to the CSPs and CSP products most regularly required by investigators. The fact that certain CSPs or CSP products are not subjected to mandate does not mean they should not be made available in respect of a lawfully issued Notice, where compliance with the Notice could be achieved from standard business systems or records. Per the SPoC Survey information (above), it would seem that 12 months is the most valuable retention period for data. It is important that there is a level playing field and a degree of certainty, both for the investigators and for the criminal justice system, therefore 12 months should be the retention period for all data subject of mandate.

Legislation in respect of lawful acquisition of CD. The positive effects of the current Pt1 Ch2 RIPA 2000 regime were identified by the Joint Committee examining the draft Communications Data Bill in 2012: the JC visited one CSP (EE) and one law enforcement agency Single Point of Contact (The Metropolitan Police Service) and it would seem were impressed with the SPoC system in terms of it professionalism in, not only the Guardian and Gatekeeper role, but also in terms of its operational effectiveness. It is widely acknowledged in law enforcement that asking the right question minimizes collateral intrusion by specific focus on material benefit sought (and likely to be achieved) by the investigators. Future legislation should look to preserve the benefits of the current regime, but where possible could encourage collaboration between CSPs and law enforcement on ways to achieve material benefit sought, whilst minimizing collateral intrusion and resultant impact on the right to an expectation of privacy.

Independent oversight, rather than independent authorisation: the benefits of independent oversight were explained to the JC in the evidence of Sir Paul Kennedy, then Interception of Communications Commissioner. In practice, Senior Responsible Officers in the agencies concerned take most seriously the recommendations of the Commissioner's staff that are undoubtedly effective in their regime of inspection. The Commissioner's Annual Report to the Prime Minister is made public and should therefore continue to provide transparency and reassurance to the public. The Investigatory Powers Tribunal provides an additional oversight function. Perhaps more subtly, the courts – in particular, the Crown Court and the Coroner's Court provide a degree of detailed scrutiny, which, though public in nature is not generally publicized. Conversely, it is felt that independent authorization would add little benefit to the current regime of authorisation by a senior officer independent of the

investigation: investigations into, for example, crimes in action and vulnerable missing persons are, by their nature, fast moving and very often driven by iterative enquiry, where the answer to one question precipitates posing the next question: it is vital to the expedience of such investigations that they are not impeded by administrative delay. It is strongly felt that the balances in the oversight regime counter any perception of potential misfeasance in the current regime for lawful acquisition.

A specialist accredited workforce with mandated training and continual professional development. The effective use of communications data as an investigative and evidential capability and the requirement to achieve substantial material benefit to specific investigations relies on a skilled workforce in the Single Point of Contact – all SPoC staff members receive training which results in their accreditation to perform the functions of their role. In order to maintain their effectiveness in performance of their Guardian and Gatekeeper duties, it is imperative that SPoCs attend mandated training on an annual basis. Attention to detail ensures that 'asking the right question first time' minimizes collateral intrusion and assures the proportionality of each lawful acquisition.

Best practice in CD investigation is focused on asking the 'smart' question in a given operational scenario. The fragmentation of data, due to mobile interoperability will mean that in future, the smart question will not be as readily identifiable, the consequent compound and iterative enquiries that will necessarily follow, where investigators attempt to determine, for example, devices present at two or more locations within given date and time parameters could potentially, quite lawfully, result in substantial amounts of data being collected which is of minimal benefit to the investigation, coupled a very small amount of data which has high value. The 'smart question' approach would allow the processing of data to answer the compound question – i.e. I am investigating a three-scene murder: murder scene, body deposition site and scene of burnt out car used in commission of the murder – question: what device was at all three scenes between given dates and times? Separately considered, such questions could generate large data-sets, but considered together, could deliver one answer. This was the premise behind the Request Filter clause in the draft CD Bill. It was broadly welcomed on the basis that observers could see the potential to assist with efficient and effective police response and equally it was clear that collateral intrusion could be effectively managed 'upstream' from the investigators. Law enforcement would be keen to have a legal

framework that encouraged such activity on the basis of the benefits to public protection and the prevention and detection of crime and equally, from a privacy perspective, there must be positives to be drawn out from such an approach.

Clarification of the law in relation to jurisdictional matters: it would be extremely helpful to law enforcement to have clarity on internet or 'cloud' storage – whether webmail, or simple cloud data storage. One doctrine which seems to be gathering some momentum in Europe is the idea that the point of access to data is the point at which the data can lawfully be acquired – in other words, if I am a webmail user, then the point at which I access my webmail is the place where my webmail data are stored.

Question 7 - 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?

Throughout Europe and in the United States, Canada, Australia and New Zealand, the threats and risks are broadly similar; law enforcement methodology is largely similar and the only really significant areas of difference are where national law and policy vary from those in the UK.

- All of the developed countries (including those from the US) cite difficulties with obtaining CD from CSPs in the US;
- There is no mandatory data retention by CSPs in many of the friendly countries outside the EU;
- CD is in some cases seen as a precursor activity to obtaining warranted LI;
- There is some evidence to suggest that, even in countries (such as the US) where LI product is admissible in evidence, that there is increasing reliance on CD;
- The FBI broke cover with their 'Going Dark' initiative (http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies): the significance of this is two-fold – firstly, there is a cogent analysis of the capabilities gap, characterized by changes in communications technology and inability of

some CSPs to comply with Court Orders; secondly the question is raised regarding the fitness for purpose of existing legislation. This article was pre-Snowden, but the issues exposed still apply, albeit exacerbated by the Snowden revelations:http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html

- The Australian government was unsuccessful in passing data retention legislation in 2013.
- Dutch colleagues, in recognition of the benefits of the invalid Data Retention Directive, have indicated they would support the case for a replacement. It is likely that colleagues elsewhere in Europe would similarly support such a development.
- The UK has probably the oldest and best-established deregulated market, promoting a thriving innovative communications industry. The inter-dependency of niche service providers who specialise in providing specific, often tailored, communications services creates an environment where SPoC staff are continually evolving strategies to assist investigators: in turn the robust nature of the SPoC system is the envy of many friendly countries, without dedicated professional staff, trained and equipped for work in this area.
- The competitive nature of the UK telecommunications industry means that, while there are some certainties, mergers and acquisitions can affect any of the 'core' companies and to a greater extent, the start-ups smaller companies. Whilst this can have the effect of exacerbating the issues explained above, competition can create some anomalies which might not be recognised by colleagues from other jurisdictions. For example, the network subsidisation of handsets in the UK led to a massive uptake in smartphone utilisation, with the effect that, because subjects of law enforcement enquiry are part of the consumer community, the UK is ahead of the curve that would be recognised either later or to a lesser extent in many other countries.

I would welcome the opportunity to discuss matters further to meet your requirements.

Report Prepared by M Atkinson and D Johnston

September 2014

The Bar Council

RIPA, DRIPA and the protection of Legal Professional Privilege

I write on the subject of legal professional privilege (LPP) and its protection in the context of the State's information-gathering activities; that is, broadly, the powers governed by the Regulation of Investigatory Powers Act 2000 (RIPA). Specifically, a series of events have brought into sharp focus the lack of protection for privileged communications between lawyers and their clients under the current legislative framework.

Against that background, the Bar Council has publicly reiterated its call for assurances from Government that measures will be introduced to protect LPP. Specifically, the Bar Council is renewing its call for amendment of the law and policy governing these activities. I will write to the Attorney-General inviting his support for that initiative. I am conscious that you also have an interest in this area, having been tasked earlier this year with the Investigatory Powers Review. I recognize that this letter comes rather later than the 3 October cut off date announced for evidence to that Review. However, the issue is an important one and I hope that you will be able to take into account the Bar Council's views in preparing your report on the Review, and more generally in the course of your role as Independent Reviewer.

I know that you will need no reminder of the fundamental importance of LPP to the administration of justice. The privilege is that of the client, not the lawyer. It is a cornerstone of a society governed by the rule of law that persons are able to consult a legal adviser or representative in absolute confidence, knowing there is no risk that information exchanged between lawyer and client will become known to third parties without the client's clear authority. That is of particular importance where individuals come into contact with the criminal justice system. The possibility of privileged information leaking to the investigating or prosecuting authorities creates an obvious and serious danger of miscarriage of justice. As you will of course appreciate, LPP does not, extend to communications made with the intention of furthering a criminal purpose -the "iniquity exception". Subject to that, however, it is the responsibility of the State to recognise and protect LPP.

In 2011, the Bar Council notified the Government that it had serious concerns that RIPA in its present form violates LPP by enabling the authorities secretly to obtain information about private communications between lawyer and client. RIPA makes no mention of LPP, but the need for reform of RIPA became apparent in

2009 when the House of Lords decided *In Re McE*[1] a Northern Ireland appeal. The House held that Part 2 of RIPA permits the covert surveillance of meetings between defendants and their lawyers, even though no express provision of the Act authorises it. The *McE* decision applies equally to the other covert investigation techniques governed by RIPA: interception of communications, acquisition of communications data and use of a Covert Human Intelligence Source (CHIS).

The issue of LPP was never debated by Parliament when RIPA was enacted. The Lords' decision is unusual in taking the *absence* of express provision as authorising officials to override important rights protected by the common law, in contrast to the usual "principle of legality" recognised in such cases as *R v Secretary of State for the Home Department, Ex p Simms* [2000] 2 AC 115. The present state of affairs lacks clarity and has grave implications for the administration of justice.

In the wake of *In re McE* the Bar Council participated in the Home Office consultation exercise on amendment of certain of the Codes of Practice issued under RIPA. But it quickly became plain that changes were needed to primary legislation. In 2011 the Government introduced the Protection of Freedoms Bill which proposed a number of amendments to RIPA. We urged Government to take that opportunity to make the changes necessary to provide proper protection of LPP. We sponsored carefully framed and measured amendments in the Lords, the effect of which would have been to amend the provisions of RIPA to:

- Prevent the authorities from deliberately using the RIPA powers of surveillance, covert human intelligence sources (CHIS), interception of communications and acquisition of communications data to target legally privileged information

- Continue to permit the authorities to seek access to privileged information where the lawyer-client relationship is being abused for a criminal purpose, and

- Make provision, through the RIPA Codes of Practice, for minimising the risk of the authorities accidentally obtaining legally privileged material and setting out the steps to be taken when that happens.

Regrettably the Government's response was to reject our proposed amendments. Since then the Bar Council has also responded to further periodic consultations on certain of the Codes of Practice, but our suggested improvements have likewise not been taken up.

[1] [2009] 1 AC 908 - http://www.publications.parliament.uk/pa/ld200809/ldjudgmt/jd090311/mce-1.htm

In the meantime, and in particular in 2013-14, there has been a series of most troubling reports about State activities and the continued threat to LPP and confidential information.

These include recent media reports on the Investigatory Powers Tribunal proceedings involving the al Saadi and Belhadj families, which have confirmed that the intelligence agencies treated RIPA as allowing them to spy on conversations between lawyers and clients. MIS, Ml6 and GCHQ policies, which have been disclosed in the context of the case, suggest that the intelligence agencies have been targeting communications between clients and lawyers which are subject to LPP, and that these internal policies were inconsistent with even the minimal recognition which the Codes of Practice on Surveillance and use of CHIS give to LPP.

Also troubling in this regard is the finding of Mark Ellison QC, in the Stephen Lawrence Independent Review of 2014 that an undercover officer deployed into an activist group engaged with the Lawrence family campaign inappropriately met with a police officer assisting the Metropolitan Police Service in formulating its submissions to the Lawrence inquiry.

Significantly, there have also been the disclosures of Edward Snowden concerning the vast capacity of the UK (and US) authorities to undertake not only interception of communications but also bulk acquisition of internet and communications data. It is now well understood that communications data can disclose a great deal of information about the who, when and where of communications from which the authorities can build a vivid picture of the nature and circumstances of the matters communicated. In the case of lawyer-client communications, data can reveal not just the fact of lawyer-client contact but a good deal of information about the context and, by inference, significant elements of the content. The acquisition, retention and processing of such data therefore directly engages LPP. While LPP, for the reasons summarised above, is in a special category, we wish to make plain that we also have concerns about the effect of the current legal regime as regards the authorities' access to other categories of confidential information about communications. It is particularly troubling that the police have used data acquisition powers under RIPA to sidestep the protection given by the Police and Criminal Evidence Act 1984 to journalistic communications, thus enabling the authorities to identify the confidential sources of journalists. Journalistic activity is often of crucial importance in preventing and uncovering miscarriages of justice.

The legislative approach to communications data is primarily contained in RIPA and the Data Retention and Investigatory Powers Act 2014 (DRIPA). As you know, the latter empowers the Secretary of State to issue a data retention notice to telecommunications services providers, requiring them to retain certain data types for up to 12 months. It will in turn be amended by the enactment of the Counter-Terrorismand Security Bill, which would further enable the Secretary of State to require providers to retain the data that would allow relevant authorities to identify the individual or the device that was using a particular internet protocol address at any given time.

In his November 2014 letter to the President of the Law Society and myself, James Brokenshire MP, Minister for Immigration and Security, accepted that access to communications data relating to certain kinds of contact, including between lawyers and clients, can be particularly sensitive. However, he did not accept that communications data itself is subject to any form of professional privilege. We believe that response cannot be sustained when one considers the array of data now available to government agencies and the cumulative effect of what that they may reveal.

It is in those circumstances that the Bar Council has renewed its call (made by letter to Mr Brokenshire MP of 24 October) that the Government provide assurance that measures will be introduced to protect the legal privilege between lawyer and client.

Specifically, the Bar Council is renewing its call for primary legislation to create proper and robust safeguards for LPP together with amendment of the Codes of Practice under RIPA. I attach a copy of the proposed amendment to RIPA, contained in a briefing paper to peers which the Bar Council prepared during the Lords Report Stage proceedings on the Protection of Freedoms Bill. We are also preparing suggested amendments to the Codes of Practice, including the Code on Acquisition and Disclosure of Communications Data, to ensure that the Codes provide considerably strengthened protection for LPP pending changes to the primary legislation. None of these proposed reforms would in any sense compromise the important public interest in preventing and detecting serious crime, including acts of terrorism. The iniquity exception is entirely adequate to prevent those with criminal intent from abusing the lawyer-client relationship to further their unlawful objectives.

In that spirit I would invite you, in completing your Investigatory Powers Review and undertaking your review functions generally, to examine the relationship between the current legal and policy framework and LPP, with a view to making recommendations for the adequate protection of LPP across the whole range of information-gathering powers governed by RIPA, DRIPA and the Counter-Terrorism and Security Bill. If you feel that the Bar Council could contribute to that exercise, then please do not hesitate to ask and we will be happy to assist in any way we can.

Nicholas Lavender QC,

Chairman of the Bar 2014

December 2014

PROTECTION OF FREEDOMS BILL

HOUSE OF LORDS REPORT STAGE

New Clause proposed by the Bar Council of England and Wales for the protection of legal professional privilege

Introduction

The Bar Council has serious concerns that the Regulation of Investigatory Powers Act 2000 (RIPA) in its present form violates legal professional privilege (LPP) by enabling the authorities secretly to obtain information about private communications between lawyer and client. RIPA makes no mention of LPP, but the power to override LPP was revealed by a 2009 judicial decision of the House of Lords. The issue was never debated by Parliament when RIPA was enacted. The present state of affairs lacks clarity and has grave implications for the administration of justice. The Protection of Freedoms Bill is designed to redress the balance between citizen and State in relation to exactly this kind of issue. The proposed New Clause would make a careful and measured amendment to RIPA which, consistent with the aims of this Bill, would:

- Prevent the authorities from deliberately using the RIPA powers of surveillance, covert human intelligence sources (CHIS), interception of communications and acquisition of communications data to target legally privileged information

- Continue to permit the authorities to seek access to privileged information where the lawyer-client relationship is being abused for a criminal purpose, and

- Make provision, through the RIPA Codes of Practice, for minimizing the risk of the authorities accidentally obtaining legally privileged material and setting out the steps to be taken when that happens.

Background

1. The right of a person in custody to private consultation with a lawyer is expressly protected in statute. Section 58(1) of the Police and Criminal Evidence Act 1984 (PACE) declares: ‚A person arrested and held in custody in a police station or other premises shall be entitled, if he so requests, to consult a solicitor privately at any time.'
2. The importance of an accused being able to confer with their lawyer in private has also been emphasised in numerous cases on the ECHR, decided in the UK and in Strasbourg. Former Lord Chief Justice Lord Taylor summed up the importance of LPP when he observed that:

   ‚... a man must be able to consult his lawyer in confidence, since otherwise he might hold back half the truth. The client must be sure that what he tells his lawyer in confidence will never be revealed without his consent. Legal professional privilege is thus much more than an ordinary rule of evidence, limited in its

application to the facts of a particular case. It is a fundamental condition on which the administration of justice as a whole rests.'[1]

3. The need for reform of RIPA became apparent in 2009 when the House of Lords decided *In Re McE,*[2] a Northern Ireland appeal. The House held that Part 2 of RIPA permits the covert surveillance of meetings between defendants and their lawyers, even though no express provision of the Act authorises it and despite the careful protection of LPP by PACE. The *McE* decision applies equally to the other covert investigation techniques governed by RIPA: interception of communications, acquisition of communications data and use of a CHIS.

4. Section 27 of RIPA provides that

'Conduct to which this Part applies shall be lawful for all purposes if (a) an authorisation under this Part confers and entitlement to engage in that conduct on the person whose conduct it is; and (b) his conduct is in accordance with that authorisation.'

5. Significantly, and as a sign of the lack of clarity inherent in the current regime, the judges were not of the unanimous view that section 27 of RIPA 'trumps' section 58 of PACE. Lord Phillips of Worth Matravers dissented, observing (at paragraph 41):

'While RIPA enables authorisation of surveillance of communications to which LPP attaches at common law it does not, in my view, enable authorisation of invasion by covert surveillance of the express rights given by statute to a detainee to consult a lawyer privately. It would not be incompatible with the Convention for power to be granted in exceptional circumstances to carry out such surveillance, but I consider that the power should be granted by a statute that adequately defined those circumstances and prescribed who was to ascertain that they existed.'

6. Lord Phillips summarised the importance of LPP at paragraph 45 when he said that 'The rationale for LPP is that it is necessary if clients are not to be inhibited from being frank with their lawyers.' His Lordship stated that the concern of the

---

1 *R v Derby Magistrates' Court, Ex p B* [1996] AC 487, 507.

2 [2009] 1 AC 908 - http://www.publications.parliament.uk/pa/ld200809/ldjudgmt/jd090311/mce-1.htm

client in these circumstances is that the communication may be disclosed and then used to his detriment. If the state is able to eavesdrop on legitimately privileged communications for the sake of gathering intelligence, there will be an inevitable 'chilling effect' upon clients, who will feel unable to speak openly with their lawyers. This would seriously undermine the fundamental human right afforded by LPP.

7. Recent high-profile cases involving use of CHIS have emphasised the need for LPP to be explicitly protected. Undercover police officers PC Mark Kennedy and DC Jim Boyling, infiltrating protest groups pursuant to RIPA authorisations, maintained their cover while fellow protesters were prosecuted and tried for offences. In Kennedy's case (*R v Barkshire & Others)*, 'significant non-disclosure' of his role led to 20 overturned convictions and cases dropped against six other campaigners.

8. The present Lord Chief Justice, Lord Judge, expressed disquiet that an undercover police officer may have been party to legally privileged communications between the defendants and their lawyers. The concerns of the Lord Chief Justice were confirmed in the case of DC Boyling (*R v Jordan*), when it emerged that DC Boyling had indeed attended meetings with the defendant and his solicitor.

9. The *Barkshire* and *Jordan* cases demonstrate the serious problems likely to arise when persons acting under RIPA authorisations obtain access to privileged information. This is not simply a privacy or confidentiality issue: there are wider concerns about fair trial when serving police officers covertly access privileged information and are in a position to pass it on to the Crown.

10. The Bar Council's concerns extend beyond the criminal law. An individual who is bringing a civil action against the state could at the same time be subject to surveillance by the state. This could be in circumstances where there is no basis for supposing that the individual is pursuing some criminal purpose rather than genuinely seeking advice on his civil claim. That prospect, in the light of the rationale for LPP articulated by Lord Phillips, is chilling.

11. The previous Government gave a partial response to *In re McE* by making two orders under powers contained in RIPA. One order concerned directed surveillance,[3] the other CHIS.[4] The orders alter the authorisation procedures where the authorities seek to target legally privileged communications. There were also revisions to the Codes of Practice.[5]

12. These 'safeguards' supposedly provided by these instruments are insufficient. The Code of Practice dealing with covert surveillance provides for the violation of LPP

---

3 http://www.legislation.gov.uk/uksi/2010/461/introduction/made

4 http://www.legislation.gov.uk/uksi/2010/123/introduction/made

5 http://www.legislation.gov.uk/uksi/2010/462/introduction/made
http://www.legislation.gov.uk/uksi/2010/463/introduction/made

only in ‚exceptional and compelling circumstances'. However, the test set out in the Code for the authorisation of surveillance that is *likely but not intended* to acquire privileged information is identical to the statutory test for any authorisation for intrusive surveillance under RIPA; it contains no special protection for privileged material. Where surveillance is *intended* to acquire privileged information, the Code stipulates that authorisation should be granted only in a restricted range of cases, such as where there is a threat to national security or to ‚life or limb'. In our view, the phrase ‚threat to life or limb' lacks clarity, and while it may catch serious intentional offences of personal violence, it could extend to more minor offences where physical injury results from lack of reasonable care or from breach of a duty that gives rise to strict liability.

13. The real difficulty, however, is that these changes do not address the fundamental point that covert investigatory powers should not be used to target privileged communications. The 'status quo' should, in our view, be the protection of LPP in all but those circumstances in which legal privilege is being abused for criminal purposes. In any event, the orders do not apply to interception of communications and acquisition of communications data.

14. It is a pity that the Government has so far declined the opportunity of the Protection of Freedoms Bill to remedy this defect in the law. At the Bill's Second Reading in the House of Commons, the Home Secretary stated:

'The Bill gives us a chance to roll back the creeping intrusion of the state into our everyday lives, and to return individual freedoms to the heart of our legislation. Under the last Government, we saw a steady erosion of traditional British liberties and a slow march towards authoritarian government. They presented us with a false choice between our future security and our historic liberties, disregarding any notion of balance between the two.'

15. In our view, the erosion of the right to legal privilege is one such ‚erosion of traditional British civil liberties' which must be addressed within this important piece of primary legislation. It will not be sufficient to tweak existing codes of conduct, all of which operate on the assumption that RIPA allows LPP to be violated for investigatory purposes.

16. In Grand Committee, the Minister pointed out that that ‚no-one can regard themselves as beyond the law or immune from investigation or prosecution'. The Bar Council respectfully agrees. Our proposal would not place anyone beyond the law. The New Clause preserves what is generally known as the ‚iniquity exception': privilege does not attach to information held, or communications made, in furtherance of a criminal purpose. More importantly, the New Clause simply brings RIPA into line with other legislation.

17. It is significant that RIPA contains no express provision about privilege, so the issue was not debated when the legislation was considered in Parliament. Instead, a significant departure from existing law came about not through open debate and

votes by both Houses, but by the retrospective application of rules of statutory construction.

18. Whenever Parliament *has* had an opportunity to consider LPP, it has consistently voted to protect it, subject to provisions (like those we propose) that prevent the abuse of privilege for a criminal purpose. Any extension beyond these powers needs to be openly debated in Parliament and in public.

19. In addition to PACE, Parliament decided to protect LPP in Part 3 of the Police Act 1997, which provides authority for property interference to carry out surveillance. Several elements of our draft Clause are based directly on that Act.

20. The Minister also referred in Grand Committee to the 2010 decision of the Northern Ireland High Court (Application of RA),[6] arguing that the court had been satisfied with the safeguards afforded by the revised Surveillance Code of Practice. But the court only dealt with the issue of safeguards in relation to the subsidiary question of how material collected from surveillance should be retained and eventually destroyed. On the central issue of whether the police could properly conduct surveillance during meetings between the applicant and his solicitor, the High Court ruled – not surprisingly – that it was bound to follow *In re McE*. If anything, this case emphasises the importance of Parliament addressing the question of LPP.

The Bar Council therefore invites Peers to support the following New Clause.

The Bar Council's proposed New Clause – Covert investigations: legally privileged material

After Clause 38

Insert the following New Clause—

Matters subject to legal privilege

Investigatory powers: legal privilege

(1) In section 5 of the Regulation of Investigatory Powers Act 2000 (interception with a warrant), after subsection (6) insert—

"(7) But an interception warrant does not authorise conduct undertaken for the purpose of doing anything in relation to—

(a) a communication, insofar as the communication consists of matters subject to legal privilege;

(b) communications data, insofar as the data relate to the communication of matters subject to legal privilege.

[6] http://www.bailii.org/nie/cases/NIHC/QB/2010/99.html

(8) In subsection (7), ‚matters subject to legal privilege' means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include a communication made with the intention of furthering a criminal purpose.

(9) For the purposes of this section the Secretary of State may by regulations make provision for the determination (on an application for an interception warrant or otherwise) of the question whether, in any case, a communication is made with the intention of furthering a criminal purpose.

(10) A code of practice issued under section 71 may in particular contain provision about—

(a) the steps to be taken to minimise the risk of conduct undertaken pursuant to an interception warrant resulting in accidental acquisition of a communication, or communications data, falling within subsection (7);

(b) the steps to be taken if it appears that such conduct has accidentally resulted in acquisition of such a communication or data.'

(2) In section 22 of that Act (obtaining and disclosing communications data), after subsection (9) insert—

"(10) An authorisation or notice under this section does not authorise or require anything to be done for the purpose of obtaining or disclosing communications data relating to the communication of matters subject to legal privilege.

(11) In subsection (10), ‚matters subject to legal privilege' means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include a communication made with the intention of furthering a criminal purpose.

(12) For the purposes of this section the Secretary of State may by regulations make provision for the determination (on an application for an authorisation or otherwise) of the question whether, in any case, a communication is made with the intention of furthering a criminal purpose.

(13) A code of practice issued under section 71 may in particular contain provision about—

(a) the steps to be taken to minimise the risk of accidentally obtaining or disclosing communications data falling within subsection (10) in the course of anything done under this section;

(b) the steps to be taken if it appears that anything done under this section has accidentally resulted in such data being obtained or disclosed."

(3) In section 27 of that Act (authorised surveillance and human intelligence sources), after subsection (4) insert—

"(5) An authorisation under section 28 or 32 does not authorise surveillance for the purpose of obtaining information about—

(a) anything taking place on so much of any premises as is in use for the purpose of legal consultations, or

(b) matters subject to legal privilege.

(6) An authorisation under section 29 does not authorise any activities involving conduct of a covert human intelligence source, or the use of such a source, for the purpose of—

(a) obtaining matters subject to legal privilege,

(b) providing access to any matters subject to legal privilege to another person, or

(c) disclosing matters subject to legal privilege.

(7) In subsection (5), ‚legal consultation' means—

(a) a consultation between a professional legal adviser and his client or any person representing his client, or

(b) a consultation between a professional legal adviser or his client or any such representative and any other person made in connection with or in contemplation of legal proceedings and for the purpose of such proceedings,

except in so far as the consultation consists of anything done with the intention of furthering a criminal purpose.

(8) In subsections (5) and (6), ‚matters subject to legal privilege' means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include anything done with the intention of furthering a criminal purpose.

(9) For the purposes of this section the Secretary of State may by regulations make provision for the determination (on an application for an authorisation or otherwise) of the question whether anything referred to in subsection (7) or (8) is done with the intention of furthering a criminal purpose.

(10) A code of practice issued under section 71 may in particular contain provision about—

(a) the steps to be taken to minimise the risk of conduct undertaken in reliance on this Part accidentally resulting in information of a kind mentioned in subsection (5) being

obtained or in any of the things mentioned in subsection (6)(a), (b) or (c) being done;

(b) the steps to be taken if it appears that such conduct has accidentally resulted in such information being obtained or such things being done."

Explanatory note on the wording of the New Clause

1. RIPA is a complex piece of legislation. Its complexity is reflected in the New Clause. As a result, this briefing paper is lengthier than would normally be expected for a single Clause.

2. The New Clause inserts new provisions into the three sections of RIPA which deal with the main covert investigatory techniques governed by that Act, namely: interception of communications pursuant to a Secretary of State's warrant (Part 1 Chapter 1); acquisition of communications data pursuant to an authorisation (Part 1 Chapter 2); and CHIS/directed surveillance/intrusive surveillance (Part 2).

3. These new provisions would operate by preventing the *targeting* of legally privileged material. It would be impermissible for a warrant or authorisation to enable any actions for the *purpose* of obtaining privileged information.

4. The obtaining of privileged information cannot be removed entirely from the scope of authorisation because, as pointed out by the Lords in *Re McE*, it may only become apparent to the authorities that privileged information has been obtained once they have received the fruits of the operation. Instead, the new Clause uses the Codes of Practice issued under RIPA section 71 as a vehicle for guidance on minimising the risk of accidently obtaining legally privileged material and dealing with the consequences of having obtained it.

5. The provisions all define ‚matters subject to legal privilege' by cross-referring to Police Act 1997 section 98(2), (3) and (4). That is the approach taken by the Government in the Covert Human Intelligence Sources: Matters Subject to Legal Privilege Order 2010.

6. The 1997 Act's exceptions from LPP have been adjusted for the purpose of this New Clause. Section 98(5) of that Act takes matters out of LPP if the item or communication in question is (a) ‚in the possession of a person who is not entitled to them' or (b) ‚held, or… made, with the intention of furthering a criminal purpose.' Here, however, the first of these exceptions would be counter-productive because a CHIS – somebody in the position of PC Kennedy or DC Boyling – is plainly *not* entitled to the privileged information, yet it is precisely in this situation that LPP needs to be preserved. So the Clause focuses on the ‚iniquity exception' of criminal intention.

7. Included in the Clause is provision enabling the Secretary of State to make regulations to determine the application of the iniquity exception. That question

would most likely arise on an application for authorisation, where the authorities have grounds to suspect that privilege is being abused. But it might also arise later in an investigation when the fruits of the covert operation are found to include lawyer-client communications which it appears might attract the iniquity exception. Hence the "or otherwise" wording. However, those subsections expressly confine the regulations to providing for determinations for the purposes of the relevant section of RIPA. So a decision about the iniquity exception under these provisions could not determine any equivalent issue arising in, for example, a criminal trial.

8. Under RIPA section 78, regulations made by the Secretary of State are subject to the negative resolution procedure (see s. 78(4)). The Bar Council feels that this is sufficient for a provision like this, which essentially establishes procedures rather than affecting substantive rights.

9. Because Chapter 1 of Part 1 of RIPA employs the concept of ‚related' communications data – that is, data related to an intercepted communication -- the insertion into section 5 of RIPA refers to communications data as well as interception. By contrast, Chapter 2 of Part 1 provides a free standing power to obtain communications data unrelated to interception. The insertion into section 22 reflects this.

10. The insertion into section 27 deals with directed and intrusive surveillance as well as CHIS. The wording defining what cannot be targeted by a CHIS (new subs. (6)) is borrowed from the Covert Human Intelligence Sources: Matters Subject to Legal Privilege Order 2010.

11. The wording of the provision about surveillance follows evidence from solicitors that legal consultations in cases involving protest or other multiple-defendant situations often take place in private premises or elsewhere. So it covers any premises insofar as they are used for legal consultations. In contrast, the Extension of Authorisation Provisions: Legal Consultations Order 2010 is limited to a restricted range of premises (e.g. prisons and police stations). The definition of 'legal consultations' used (new subsection (7)) is, however, very similar to the definition in that Order.

Dr Paul Bernal

This submission is made in response to the Investigatory Powers Review Call for Evidence, dated 21st July 2014. I am making this submission in my capacity as Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School. I research in internet law and specialise in internet privacy from both a theoretical and a practical perspective. My book, *Internet Privacy Rights: Rights to Protect Autonomy,* was published by Cambridge University Press, in March 2014 – building from my PhD, completed at the LSE. As such, I am, at least relatively speaking, an expert in the subject of internet privacy: the subject lies precisely within my academic field.

The call for evidence looks at a number of issues:

- Current and future threats, capability requirements and the challenges of current and future technologies;
- The safeguards to protect privacy;
- The implications for the legal framework of the changing global nature of technology;
- The case for amending or replacing the legislation;
- The statistical and transparency requirements that should apply; and
- The effectiveness of current statutory oversight arrangements.

1 Introduction

This response deals primarily with the privacy aspects of these issues – in particular, the safeguards needed to protect privacy. There are a number of points that need to be considered in relation to the overall debate over investigatory powers. If appropriate answers to the questions raised by these issues are to be found, the starting point has to be to ensure that the debate takes place on appropriate terms. When expert information is passed on first to politicians and other policy-makers and then to the public, both the policy-makers and the public should be, insofar as it is possible, in a position to make appropriate judgments. At present, it appears that this is not the case: much of the political debate appears to be ill informed, and public opinion is confused.

That is critically important: politicians need to have a better understanding in order to make appropriate decisions, while the public needs to be informed enough to be able to trust that what is happening is appropriate. It is not enough for the authorities just to say 'trust us': the public needs to know that they can trust the authorities. Recent events, from the Snowden revelations to a series of police-related scandals (from the various issues surrounding 'Plebgate' to undercover police officers using dead children's identities and having sexual relationships with activists they were targeting, amongst other incidents - most recently the use of RIPA to examine journalists' communications data[1]) have undermined that trust.

[1] See for example http://blogs.ft com/david-allen-green/2014/09/03/ripa-requests-plebgate-and-journalistic-sources/ and http://www.thetimes.co.uk/tto/news/medianews/article4223059ece?shareToken=67c07ad014c843da38c462e92304872a

2 Clarification of issues and framing of debate

In order to make the debate more realistic, there are a number of issues that need to be clarified:

1) That surveillance impacts upon rights other than the right to privacy. Characterising the balance to be found as one between 'individual privacy' and 'collective security' is misleading and inappropriate – and yet this is often the way that it is presented, for example by the Intelligence and Security Committee itself.
2) That privacy invasion – and the impact of surveillance – happens at the data gathering stage, not at the data access stage. At present, much of the debate seems to assume that gathering and holding data is automatically acceptable, and that controls need only be placed over access to the gathered data. There are moral, legal and practical reasons why this is not the case.
3) That practical examples of how the surveillance works need to be presented, not just technical details and legislation. For example, are people's web-browsing activities going to be monitored – and if not, how will communications data concerning webmail be gathered? What is intended concerning social networking sites? All this was subject to discussion amongst experts after the passing of DRIP – but even the experts could not come to clear conclusions. If experts are not clear, how could politicians or the public be clear?
4) That legislation needs to be detailed and limited, rather than vague and open ended. Where there are loose ends or areas open to interpretation, evidence seems to suggest that authorities will interpret in ways that suit them. The Metropolitan Police's use of RIPA to gather the telecommunications data of Tom Newton Dunn, political editor of the Sun, as noted above, is a recent case in point, but is just one of many examples.
5) That oversight needs to be more transparent, independent and accountable. The current system, at the surface at least, does not seem to function. The 'public' meeting of the ISC in November 2013 did not provide the kind of public assurance that is needed – indeed, it suggested precisely the opposite. The key questions were not asked, and it looked very much as though the witnesses had been prepared for the committee. It looked, unfortunately, like public theatre rather than independent oversight. Moreover, it did not appear as though the committee members had either the expertise or the intention to hold the heads of MIS, MI6 and GCHQ to account. That should be their job.

The result of all these, in relation to the key issues raised in the call for evidence, at least insofar as privacy is concerned, is that the case for changing the law is a strong one, and that this change should be set out to ensure greater protection for privacy. The starting point for that change is a shift from the 'gather all, control access' basis to a system based on targeted gathering where that targeting governed by warrants or equivalent independent oversight. Moreover, the constantly developing technological world should suggest that laws need regular review – such reviews being set out in a way to provide further independent oversight.

3 New surveillance in a new context

The kind of surveillance that currently appears to be undertaken – and was envisaged in legislation such as the Communications Data Bill in 2012 – is qualitatively different from that hitherto imagined. It is not like 'old-fashioned' wiretapping or even email interception – and that means that the debate about it, the legislation that governs it and the oversight required for it has to be reconsidered.

It is not just that the surveillance itself is new: it is that the way that we use the internet makes it new. In particular the way that the internet is, for most people in what might loosely be described as developed societies, used for almost every aspect of our lives changes the coverage of the surveillance. As a consequence, by observing our internet activities, by monitoring our communications data, the level of scrutiny in our private lives is vastly higher than any form of surveillance could have been in the past. It is not just about our correspondence, but also about our movements, our friendships, our habits, our hobbies, our interests – and much more.

In particular, the growth of social networking sites and the development of profiling and behavioural tracking systems and their equivalents change the scope and of the information available. In parallel with this, technological developments have changed the nature of the data that can be obtained by surveillance – most directly the increased use of mobile phones and in particular smartphones, provides new dimensions of data such as geo-location data, and allow further levels of aggregation and analysis. Other technologies such as facial recognition, in combination with the vast growth of use of digital, online photography -'selfie' was the OED word of the year for 2013 for a reason – take this to an even higher level.

This combination of factors means that the 'new' surveillance is both qualitatively and quantitatively different from what might be labelled 'traditional' surveillance or interception of communications. This means that the old debates, the old balances, need to be recast. Where traditional 'communications' privacy was in some ways a subset of traditional privacy rights – as reflected in its part, for example, within Article 8 of the ECHR – the new form of communications has a much broader relevance, a wider scope, and brings into play a much broader array of human rights. The surveillance too is different – and the impact that it can have is different, more extensive, more multifaceted and with a greater impact on the people subjected to it.

4 Individual right to privacy vs. collective right to security?

Framing of this debate in this way – as suggested, for example, by Sir Malcolm Rifkind in his call for evidence for the Intelligence and Security Committee in December 2013[2] is fundamentally misleading.

4.1 Privacy is not just an individual right

Privacy is often misconstrued as a purely individual right - indeed, it is sometimes characterised as an 'anti-community' right, a right to hide yourself away from society. Society, in this view, would be better if none of us had any privacy - a 'transparent society'. In practice, nothing could be further from the truth: privacy is something that has collective benefit, supporting coherent societies. Privacy isn't so much about 'hiding' things as being able to have some sort of control over your life. The more control people have, the more freely and positively they are likely to behave. Most of us realise this when we consider our own lives. We wear clothes, we present ourselves in particular ways, and we behave more positively as a result. We talk more freely with our friends and relations knowing (or assuming) that what we talk about won't be plastered all over noticeboards, told to all our colleagues, to the police and so forth. Privacy has a crucial social function - it's not about individuals vs. society. Very much the opposite: societies cannot function without citizens having a reasonable expectation of privacy.

4.2 Surveillance doesn't just impact upon privacy

The idea that surveillance impacts only upon privacy is equally misconceived. Surveillance impacts upon many different aspects of our lives - and how we function in this 'democratic' society. In human rights terms, it impacts upon a wide range of those rights that we consider crucial: in particular, as well as privacy it impacts upon freedom of expression, freedom of association and freedom of assembly, and others.

a) Freedom of expression

The issue of freedom of expression is particularly pertinent. Privacy is often misconstrued as somehow in opposition to freedom of expression – blogger Paul Staines (a.k.a. Guido Fawkes) for example, suggested that 'privacy is a euphemism for censorship'.[3] He had a point in one particularly narrow context - the way that privacy law has been used by certain celebrities and politicians to attempt to prevent certain stories from being published - but it misses the much wider meaning and importance of privacy.

---

[2] See http://isc.independent.gov.uk/news-archive/december2013

[3] In testimony to the Parliamentary Joint Committee on Privacy and Injunctions in 2012

Without privacy, speech can be chilled. In Mexico, for example, at least four bloggers writing about the drugs cartels have not just been prevented from blogging - they've been sought out, located, and brutally murdered.[4] There are many others for whom privacy is crucial - from dissenters in oppressive regimes to whistle-blowers to victims of spousal abuse. The internet has given them hitherto unparalleled opportunities to have their voices heard – internet surveillance can take that away. Even the possibility of being located can be enough to silence them. The chilling effect that a lack of privacy has is real.

Internet surveillance not only impacts upon the ability to speak, it impacts upon the ability to receive information - the crucial second part to freedom of speech, as set out in both the European Convention on Human Rights and the Universal Declaration of Human Rights. If people know that which websites they visit will be tracked and observed, they're much more likely to avoid seeking out information that the authorities or others might deem 'inappropriate' or 'untrustworthy'. That, potentially, is a huge chilling effect. It should not be a surprise that the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in his report of 2013, described the link between privacy and freedom of expression as direct and crucial.

"States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; and infringement upon one can be both the cause and consequence of an infringement upon the other."[5]

b) Freedom of association and of assembly

Freedom of association and assembly is equally at risk from surveillance. The internet offers unparalleled opportunities for groups to gather and work together - not just working online, but organising and coordinating assembly and association offline. The role the net played in the Arab Spring has probably been exaggerated - but it did play a part, and it continues to be crucial for many activists, protestors and so forth. The authorities realise this, and also that through surveillance they can counter it.

A headline from June 2013 in the UK, "Whitehall chiefs scan Twitter to head off badger protests"[6] should have rung the alarm bells - is 'heading off a protest an appropriate use of surveillance? It is certainly a practical one - and with the addition of things like geo-location data the opportunities for surveillance to block association and assembly both offline and online is one that needs serious consideration. The authorities in the Ukraine recently demonstrated this through the use of surveillance of mobile phone geolocation data in order to identify people who might be protesting – and then sending threatening text messages warning those in the location that they were now on a list: a clear attempt to chill their protests.[7] Once more, this is very much not about individual privacy – it is about collective and community rights.

[4] See for example http://www.laht.com/article.asp?CategoryId=14091&ArticleId=442210
[5] La Rue, Frank (2013),'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', (United Nations)., p20
[6] http://www.bbc.co.uk/news/ uk-politics-22984367
[7] See http: //www.nytimes.com/2014/01 /22/world/europe/ukraine-protests.html? r=O

c) Prohibition from discrimination

Not only can surveillance and profiling enable discrimination – it can potentially automate it. It may be possible to determine almost any kind of detail about a person online through profiling – their age, religion, nationality, ethnic origin and so forth. Decisions and options available to a person may then be automatically controlled on the basis of that profiling – and the person involved may never even know what is happening. Those decisions have an impact – and this applies as much in relation to surveillance as it does in any other aspect of the internet.

4.3 Rights that underpin democracy

All this matters. It isn't a question of 'quaint' and 'individual' privacy, a kind of luxury in today's dangerous world, being balanced against the heavy, important and deadly serious issue of security. If expressed in those misleading terms it is easy to see which direction the balance will go. Privacy matters far more than that - and it matters not just to individuals but to society as a whole. It underpins many of our most fundamental and hard-won freedoms - the civil rights that have been something we, as members of liberal and democratic societies have been most proud of.

That means that the balancing exercise of 'privacy vs. security' need to be reassessed – and that more and stronger safeguards' for privacy are needed than might immediately be assumed if the narrower, more limited vision of what privacy means is taken.

5 Controls are required at the gathering stage

Perhaps the most important aspect of safeguarding privacy is to look at the stage at which controls are established over data gathering. The current method -the method that lies behind the concept of data retention – is to gather whatever is wanted, and then put controls in place over how the gathered data is accessed. This, I believe, is misconceived .The arguments for putting controls at the gathering rather than accessing stage can be divided broadly into four closely related and interlinked strands: moral principles, legal principles, 'surveillance effects', and technological pragmatism.

5.1 Moral principles

One of the essential principles of democratic society is the idea of trust. People should be generally assumed to be trustworthy, rather than generally assumed to be untrustworthy. Closely related to this are principles of justice including the presumption of innocence and the inappropriateness of 'guilt by association'. The idea of gathering data and holding relating to people 'just in case' someone might be involved in some kind of criminal act or conspiracy goes directly against these principles.

5.2 Legal principles

The European Court of Human Rights has been consistent in its understanding that the holding of data - as opposed to the accessing or the 'using' of that data - engages Article 8 of the European Convention on Human Rights. That is, the mere holding of data is an interference with the private life of the individual. This understanding dates back to the Leander case in 1987, prior to the kind of data gathering possible in the internet and 'big data' era - and has been continued through a series of cases to the recent declaration of invalidity of the Data Retention

Directive. It is a legal principle that corresponds to a nuanced understanding of the relationship between an individual and data that relates to them: a complex and personal relationship, one that needs respecting. The nature of that relationship means that even gathering personal data has an impact upon the individual, and hence engages Article 8.

5.3 Surveillance effects

Surveillance in itself has an impact upon people.[8] The so-called 'Panopticon effect' in particular, arises directly at the gathering rather than the accessing level. The principle of the Panopticon effect is that if someone knows that they may be observed, their behaviour will be chilled. If that person knows that data has been gathered and held, regardless of whether it has been accessed yet, their behaviour will be chilled. This chill has applies to expression, association and assembly – and has been observed from conventional surveillance by the Stasi to more recent technological surveillance.

As Garton Ash put it in *'The File'* when considering the Stasi, the Panopticon effect chills people into subservience and compliance:

"More typical were the nice couple from whom the University had rented my room. Intelligent, well-educated, well-informed through watching Western television, they nonetheless devoted virtually all their energies to their private lives, and particularly to extending, decorating and maintaining their cottage on a small lake some half-an-hour's drive from Berlin. "

The impact of more modern surveillance is detailed at length in La Rue's 2013 Report, as noted above. Further, the 'power effect' - the impact of the imbalance of power between those who have gathered data over those about whom the data is gathered - is magnified by having controls only at the accessing stage: the amount of data available for access is magnified and the potential imbalance in power created similarly magnified.

5.4 Technological pragmatism

There are risks attached to data, however it is held and whoever it is held by - this is part of the reason for the whole data protection regime. It is particularly relevant to surveillance. Data gathered by surveillance is vulnerable in all the ways that other data is vulnerable: vulnerable to misuse, to misappropriation, to hacking, to loss, to corruption and error, to what is loosely described as 'function creep'. Security services and other authorities are not immune to that vulnerability - as the leaks through Wikileaks, the revelations of Edward Snowden, the various data losses by the Ministry of Defence and others have demonstrated. In Australia, in August 2014 it was revealed that the Australian Federal police had mistakenly published highly sensitive information - including metadata - connected to criminal investigations.[9] There are similar stories in many other places around the world

Further, surveillance systems themselves are vulnerable: build a back door into a system and it is not only those who are intended to use it who can use it as a way to access that system. Install a 'black box' into an internet service provider's premises and that black box can itself be hacked and accessed.

---

[8] See for example Richards, Neil M.,'The Dangers of Surveillance.' 2013 Harvard Law Review,p1953 Available at SSRN: http//ssrn.com/abstract=223941

[9] See for example http.//www.theguardian.com/world/2014/aug/28/federal-police-mistakenly-publish-metadata-from- criminal-investigations

The implications of this are direct. The only data that is not vulnerable is data that does not exist. The only surveillance system that is not vulnerable is the surveillance system that does not exist. The logical consequence is that controls should be put at the data gathering stage, and at the monitoring stage where data is not gathered, rather than building universal systems and gathering all the data and putting the controls on the access and use of those systems and that data.

5.5 The nature of the controls

The controls should be in the form of warrants or equivalents, judicially authorised rather than 'self-authorised' by sufficiently senior members of the relevant service. This is critical for oversight and for trust – and it must be clear that oversight is properly independent, and is seen to be independent.

6 The need for clarity

Recent debates over surveillance have been characterised by a lack of clarity and transparency. When the revelations of Edward Snowden indicated at least something about the level of surveillance of communications data being undertaken, it was viewed as shocking - and each new revelation has brought further such reactions. That in itself has undermined trust: even now, it is unclear even to experts quite what kinds of surveillance are being undertaken, by whom, and for what purpose.

Moreover, the legislative processes have been unclear and confused – the process through which the Communications Data Bill was brought forward and eventually defeated was messy to say the least, while the rapid rushing through of the Data Retention and Investigatory Powers Act was something that to this observer at least brought parliament into disrepute. There was so little time for scrutiny and debate that even those who brought the bill forward did not seem to have a clear understanding of what the bill actually meant. Even now there seems to be little clarity. How the extraterritoriality of the act would function is still under dispute. Does the act cover webmail services, and if so, how? Does it cover web browsing? The answers in parliament were unclear – and this is an unsatisfactory situation.

The law needs to be much clearer – and worked through examples need to be provided, to make it still clearer. This kind of clarity is necessary for communications providers to know what is expected of them, and for policy makers to understand how to balance the various rights concerned. If it is not clear either what data will be gathered or how it might be used, how can those balances be achieved? Technical information about data types is not sufficient – how it works in reality, in pragmatic terms, needs to be made much clearer.

Further, this kind of clarity and these kinds of worked through examples can help to limit the level of 'mission creep' that can take place with this kind of legislation. It can limit the opportunity for a 'favourable' reading of potentially ambiguous wording to be made – and can protect both those undertaking surveillance and those who are subject to it. It can build trust – and trust is critically important here. Similarly, laws need to be more clearly limited: open-ended and ambiguous legislation leads to problems for all concerned.

7 The need for proper oversight

The first question about oversight that needs to be asked is about the purpose of oversight. What is the oversight supposed to be doing, and for whom? Is it to provide some kind of 'quality control' for the intelligence and security services? Is it to help politicians to understand what the intelligence and security services are doing for them? Or could it also be to keep a tighter rein on the intelligence services, to represent the

public and to prevent the intelligence and security services from exceeding their remit? We need clarity about this too – and we need to ensure that this last part of the possible function of the oversight is done. There need to be checks and balances over the activities of the intelligence and security services, and checks and balances that not only function but are seen to function.

It is hard to make an accurate assessment of how successfully the current oversight systems function, as so much of it is performed privately. The 'open evidence session' of the Intelligence and Security Committee in November 2013, however, did not inspire confidence: precisely the opposite. It was hard to conclude that it was anything but political theatre – few of the important questions were asked, the three heads of services seemed to have been prepared for the questions in advance, and the committee members seemed unwilling to ask anything difficult. It was hard to feel that the committee members even understood the issues – and that in itself was disappointing to say the least.

Of course it is difficult to have genuinely independent oversight – but it must be possible to have something better than this. Something that includes more expert observers, more independent members, more people that have a specific remit to look at the human rights angles of surveillance. These members should be drawn from a wider pool than just politicians: in particular, they should include representatives from academic and civil society. They should include people with genuine expertise in the technology and the law – if oversight is to function properly, those overseeing need to be able to understand what they are dealing with.

8 Regular review

One of the key issues raised in the call for evidence are the implications for the legal framework of the changing global nature of technology. There are two aspects even to that statement: the 'changing' aspect and the 'global nature' aspect. The way that technology changes – and that our use of that technology changes – has been addressed to an extent in section 3 above, but it needs to be recognised that many of the changes that happen are unpredictable. The global nature of technology is something that anyone who deals with the internet has to grapple with every day – and there are no simple ways to deal with it. There are two immediate implications:

1) That legislation, surveillance practice and oversight all need regular review. Laws should have built-in review mechanisms: sunset clauses or their equivalent. Just letting things 'roll over' should not be an option – it is through that kind of an approach that legislation and oversight quickly loses touch.

2) That it should be remembered that all regulation – and indeed all surveillance activities – are somewhat 'rough and ready' and that finding a 'perfect' solution is not possible. How other states deal with the internet has an impact on both people in the UK and in the activities of the intelligence and security services. This, too, puts further emphasis on regular review and proper oversight.

I hope that this contribution is of some assistance. It seems to me that if a greater degree of clarity and transparency is not reached, then the potential for misunderstanding, for excessive fears and hence even more chilling, is significant. It is in the interests of all that this is avoided.

If needed, I can provide further evidence and more extensive support for the arguments made in this submission.

October 2014

Big Brother Watch

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group that was founded in 2009. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this inquiry we have published a number of reports on the use of RIPA, for example *A Legacy of Surveillance* and *The Grim RIPA*.[1,2] We have also given evidence to both the Joint Committee on the Draft Communications Data Bill and the Home Affairs Select Committee on the use of surveillance powers by the police and intelligence agencies. Finally, we have released a paper examining ways in which the Government can improve its surveillance transparency.[3]

Summary of Key Points

- One of the greatest safeguards to privacy would be an increase in the levels of transparency around the use of surveillance powers.
- The current oversight arrangements simply aren't good enough. Both the Intelligence and Security Committee and the Commissioner system need urgent improvements.
- The claims of a capabilities gap in the collection of communications data have been greatly exaggerated.

Specified Issues

1. **Current and future threats, capability requirements and the challenges of current and future technologies.**

A number of figures, such as the Home Secretary; Theresa May MP, have argued that there is a growing gap between the amount of communications data that exist and the amount that can be accessed by law enforcement agencies.[4] This has become known as the "capability gap". The **Intelligence and Security Committee's (ISC)** 2013 report, *Access to Communications Data by the Intelligence and Security Agencies* quoted a Home Office report that estimated the potential gap at around 25%.[5] It is however an unhelpful concept and one that is not universally acknowledged as having merit. Looking specifically at the 25% figure, its' veracity was questioned during an ISC oral evidence session by the

[1] Big Brother Watch, *A Legacy of Surveillance*: http://www.bigbrotherwatch.org.uk//files/ripa/RIPA_Aug12_final.pdf
[2] Big Brother Watch, *The Grim RIPA*: http://www.bigbrotherwatch.org.uk/TheGrimRIPA.pdf
[3] Big Brother Watch, *Enhancing surveillance transparency: A UK policy framework*: http://www.bigbrotherwatch.org.uk/files/briefings/BBW_transparency_2014.pdf
[4] T. May, *Letter from Rt Hon Theresa May MP, Home Secretary, to the Chairman of the Committee*, 7th May 2014: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/563-iii/563we02.htm
[5] Intelligence and Security Committee, *Access to communications data by the intelligence and security agencies* (2013) paragraph 27, p. 11: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf

Director General of MI5, who argued that it rested on "*some pretty heroic assumptions*".[6]

Turning to the concept itself the **Joint Committee of the Draft Communications Data Bill** took issue with the idea, commenting that:

> "*Technological advances and mass uptake of internet services since RIPA was passed in 2000, including social networking sites, means that there has been, and will continue to be, a huge increase in the overall amount of communications data which is generated and is potentially available to public authorities*." [7]

The Joint Committee's final report went on to argue that part of the capability gap was down to a "*lack of ability of law enforcement agencies to make effective use of the data that is available*." [8]

Additionally, when the Metropolitan Police Service Commissioner, **Sir Bernard Hogan-Howe**, gave evidence to the **Home Affairs Select Committee (HASC)** he was asked how he would spend an additional £1.8bn (the amount then earmarked for the Draft Communications Data Bill). He identified three main areas in his response: training, community policing and IT. Elaborating, he said:

> "*Across the country policing generally spends £1.2 billion on IT. My point would be that it is more green-screen than it is iPad, I am afraid, and it does not seem to catch criminals*."[9]

The fact remains that the police already recover large amounts of data from people they suspect of committing crimes, but are unable to properly utilise it because of skills and manpower shortages.

Advances in electronic communications as well as the companies that provide them are often blamed for the capability gap. When the Prime Minister announced the **Data Retention and Investigatory Powers Act 2014 (DRIP)** he justified it, partially, by saying "*there is now a real risk that legal uncertainty will reduce companies' willingness to comply with UK law.*"[10] However there is compelling evidence to show that this is in fact a false assumption and that technology companies are not to blame for any potential capability gap.

Facebook's *Global Government Requests* report for 2013 showed that they received **1,975** data requests that specified a total of **2,337** users between January and June 2013. They complied with **1,343** of them (rejecting **632**), meaning that information was disclosed **68%** of the time. [11] Similarly Microsoft only rejected **3.1%** or **270** of the **8,617** requests that were made in 2013.[12]

[6] Ibid
[7] Joint Committee on the Draft Communications Data Bill, *First Report* (2012) paragraph 16, p. 16:
[8] Ibid p. 19
[9] Home Affairs Select Committee, *Olympics Security: Seventh Report of Session 2012-12, Volume II Oral and Written Evidence*, Q403.
[10] D. Cameron, *Transcript of the PM and Deputy PM's speech on emergency security legislation*, 11th July 2014: https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation
[11] Facebook, *Global Government Requests Report*: https://www.facebook.com/about/government_requests
[12] Microsoft, *2014 Law Enforcement Requests Report*: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

These figures support the assertion from the Joint Committee: that the problem lies not with the ability of law enforcement agencies to access the information but in their ability properly utilise it once they get it, as well as understanding the correct procedures to request it in the first place.

2. **The safeguards to protect privacy.**
3. **The statistical and transparency requirements that should apply.**

One key safeguard that can be easily implemented is an increased emphasis on transparency. The aforementioned Government data request reports produced by technology companies are a good guide to how this can be achieved. It is also something that would be supported by a large majority of UK citizens.

Polling conducted for Big Brother Watch, revealed that **70%** of British adults think British companies should publish reports on how often they receive requests for customer data from the police and security services. Additionally, **66%** said that the Government should publish more data about how surveillance powers are used.[13]

Big Brother Watch has previously advocated methods for increasing the transparency of organisations that use surveillance powers. Our paper *Enhancing surveillance transparency: A UK policy framework* argues that individual agencies should proactively publish information on their use of surveillance techniques. Ideally this would include the following:

• Where Covert Human Intelligence Sources, directed and intrusive surveillance or intercept powers have been used, for what offence and whether the investigation resulted in a prosecution or conviction.

• How much data is collected under each warrant and how many citizens were affected.

• The number of individuals affected by these requests.[14]

It is important that each agency publishes its own figures despite the temptation to leave this responsibility to an oversight body such as the **Interception of Communications Commissioner (IoCC)**. This should be avoided as bodies such as the **IoCC** should focus on ensuring that the powers are used properly and not be burdened with the additional task of providing statistical bulletins.

It is important to point out that this additional information would not compromise ongoing investigations nor would it impinge on national secure if it were made public. It would however give the public a greater insight into how often surveillance powers are used as well as their effectiveness.

Indeed the US provides examples of how to address surveillance transparency, one example being, in line with Barack Obama's assertion that the US "*can and must be more transparent*", that the Justice Department publishes annual reports on the use of wiretaps by agencies.[15] [16] Each of these reports, which date back to 1997, contains tables, text and

[13] Big Brother Watch, *Enhancing surveillance transparency: A UK policy framework*, p. 2: http://www.bigbrotherwatch.org.uk/files/briefings/BBW_transparency_2014.pdf
[14] Ibid, p. 2
[15] BBC News, *Barack Obama pledges greater surveillance transparency*, 10th August 2013: http://www.bbc.co.uk/news/world-us-canada-23642880
[16] Justice Department, *Wiretap Report 2013*: http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx

charts to properly **breakdown information about the number of authorizations and approvals** Government agencies have made. Importantly it **covers both federal and state officials** and shows information on the **interception of wire, oral or electronic communications**.[17]

Linked to this, the US already publishes **break downs of the use of powers by its intelligence agencies**. These steps are supported by the decision to release information on the **annual use of surveillance orders**.[18] This includes the "*total number of orders issued during the prior 12-month period, and the number of targets affected by these orders*."[19]

Linked to this, all organisations that are involved in surveillance activities should proactively carry out stringent auditing processes of their powers and activities. Where any kinds of infringements or related disciplinary procedures are found the information should be published.

It is of the utmost importance that the UK Government begins to follow these examples and start implementing measures that will move towards increased transparency.

Another safeguard that could be useful in this area is the proposed **Independent Privacy and Civil Liberties Oversight Board (PCLOB)**.[20] The idea is not without merit, however there are a number of concerns that should be addressed before any plans are finalised. Most importantly it should reflect its proposed title; it should be free to consider any and all legislation that could result in an infringement on privacy, not just terrorism legislation. This is particularly important as **DRIP** was passed with the rationale that it would help combat "*serious organised crime*", including child abusers as well as terrorists.[21]

This necessity is made even more important when the original Home Office Impact Assessment that was drawn up in anticipation of the EU Data Retention Directive being overturned is considered. Most notably, there is barely a mention of the impact on combating terrorism. Concern is however raised over the capacity of law enforcement agencies to tackle the following crimes: "*Murder*", "*sexual exploitation*", "*drugs*", "*door step fraud*" and "*locating vulnerable people*."[22]

Giving PCLOB the option to declassify materials, in a similar way to the **Slovenian Data Protection Authority**, would allow it to make a tangible contribution to Government transparency.[23] Thought should also be given to empowering it to decide which inquiries to

[17] Ibid

[18] TechHive, *US to release annual figures on spying orders and people affected*, 30th August 2013: http://www.techhive.com/article/2047791/us-to-release-annual-figures-on-spying-orders-and-people-affected.html

[19] Office of the Director of National Intelligence, *DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities*, 29th August 2013: http://icontherecord.tumblr.com/tagged/statement/page/3

[20] *Transcript of the PM and Deputy PM's speech on emergency security legislation*, 11th July 2014: https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation

[21] T. May, *Data Retention and Investigatory Powers Bill*, 10th July 2014: http://www.publications.parliament.uk/pa/cm201415/cmhansrd/cm140710/debtext/140710-0001.htm#14071054000003

[22] Home Office, *Data Retention Legislation: Impact Assessment*, 27th June 2014:

[23] K. Kotnik Sumah, *System of Access to Classified Information in the Republic of Slovenia*, p. 13: https://www.iprs.si/fileadmin/user_upload/Pdf/clanki/System_of_access_to_classified_information_in_the_Republic_of_Slovenia.pdf

carry out, rather than being told what it can or should investigate. This system is currently used by the **Australian Independent National Security Legislation Monitor** who can begin reviews on "*his or her own initiative*."[24]

4. **The implications for the legal framework of the changing global nature of technology.**
5. **The case for amending or replacing legislation.**

The main piece of legislation that should be examined in this area is **the Regulation of Investigatory Powers Act 2000** (RIPA).

The primary concern with the legislation is that it was passed before the launch of social networking sites such as **Facebook** (2004) and **Twitter** (2006). These sites provoked a revolution in the way in which we communicate with one another, meaning it would be unfair to expect Parliamentarians to have considered the impact of this law on entirely new platforms when it was originally scrutinised.

The outdated nature of **RIPA** has led to some concerning practices. One example was revealed as part of the legal challenge being brought against GCHQ at the **Investigatory Powers Tribunal (IPT)**. As part of his evidence **Charles Farr**, Director of the Office for Security and Counter-Terrorism revealed that messages sent via social media can be classed as "*external communications*."[25] This means that there is no need to obtain a warrant before the collection of social media messages. The rationale for this being that most social media communications are routed through servers that are often in countries such as the US, before arriving with their intended recipient. The action of collecting communications without a warrant is judged to be legal even if all parties are UK citizens and are within the UK at the time. It is instances such as this show that the law in its current state is far too open to interpretation; highlighting the need for reform.

This has been recognised by a number of public figures. In a speech in March 2014 **the Shadow Home Secretary**, **Yvette Cooper,** argued that "*significant questions remain about the way the legal framework operates and whether it is falling behind the pace of modern technology*."[26] In their report into Counter-Terrorism measures **HASC** argued that a review of RIPA was necessary and that it should include measures such as bringing the legislation "*up to date with modern technology, reduce the complexity (and associated difficulty in the use of) the legislation*."[27] As part of the announcement of DRIP, the **Deputy Prime Minister, Nick Clegg**, noted that "*there are fundamental questions to be asked about the scope of existing powers; about whether the Regulation of Investigatory Powers Act has kept pace with technology*."[28]

[24] Independent National Security Legislation Monitor Act 2010, Section 5, Part 2, Division 1, 6 (1): http://www.comlaw.gov.au/Details/C2010A00032

[25] *Witness Statement of Charles Blandford Farr on behalf of the Respondents*, Investigatory Powers Tribunal, paragraph 132, p. 40: https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness_st_of_charles_blandford_farr.pdf

[26] Y. Cooper, *The Challenges of a Digital World to our Security and Liberty*, Speech to Demos: http://press.labour.org.uk/post/78448368189/the-challenges-of-a-digital-world-to-our-security-and

[27] Home Affairs Select Committee, Counter-Terrorism, 30th April 2014, paragraph 177, p. 70: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf

[28] *Transcript of the PM and Deputy PM's speech on emergency security legislation*, 11th July 2014: https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation

It is important that as a part of this review of RIPA the definitions being used are redrawn. One example would be to include a specific definition of geo-location data. Another would be to revise the meaning of "content". As a result of current technology some communications can be private and not person-to-person, for example a status update on Facebook.

A further issue that has been identified with RIPA is the number of organisations that can utilise surveillance techniques. A UN special report drew attention to this, commenting that over 200 "*agencies, police forces and prison authorities can acquire data*". It warned that "*as a result it is difficult for individuals to foresee which State agency they might be subjected to surveillance."*[29] For this reason serious thought should be given to the number of organisations that can potentially access communications data under RIPA.

One area where serious consideration should be given to entirely new legislation is the practice of bulk or mass collection of data. Big Brother Watch has previously raised this point in evidence to the ISC. There should be an explicit statutory bar on the acquisition of bulk data relating to thousands or millions of British people, excepting situations that could reasonably be considered an emergency. It is surveillance of this nature that prompted the legal proceedings Big Brother Watch has launched against GCHQ at the European Court of Human Rights. As part of the original submission it was argued that such unchecked surveillance is a breach of the Right to Privacy under Article 8 of the European Convention on Human Rights.

Section 94 of the Telecommunications Act 1984 could also be repealed as Ministers have repeatedly failed to cite it in relation to the current activities of the intelligence services. This would therefore indicate that it is not being used and it should therefore be taken off the statute book. If it is in operation then it therefore raises the question as to why it isn't mentioned alongside legislation such as **RIPA**, the **Intelligence Services Act** and the **Human Rights Act**.

The recently announced review into the use and operation of **RIPA** is welcome and should not be a missed opportunity. It is a chance to improve how surveillance legislation is being used, with an emphasis on bringing it fully up to date with modern technology.

6. **The effectiveness of current oversight arrangements.**

This section will consider the workings of both the **ISC** and the **Commissioner system**.
This review process should be seen as an opportunity to remedy several of the failings of the ISC. In its current format the Committee a serious block to providing the oversight that is necessary to give the public confidence that surveillance powers are being used proportionately and efficiently. In order to increase its effectiveness, the following reforms should be made:

• The Chairman of the ISC should be a member of the Opposition party. Additionally, in their previous careers, they should have had a minimum amount of contact with the agencies that they are overseeing.

• The **ISC** should be made into a full Parliamentary Select Committee. This is

[29] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protectionof the right to freedom of opinion and expression, Frank La Rue* (2013), p. 15: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[29] Ibid p. 21

particularly important when considering the nomination and election of the Chairman; as with other Committees this should be a matter for Parliament.

• The staffing and the funding of the ISC should be improved. At its current level it has just 9 full time support staff. In comparison, the US **House Permanent Select Committee on Intelligence** has 32 staff members.[30]

Looking specifically at the Chairman of the ISC, it is clear that there must be an evolution as to who is eligible for selection, as well as the process of selection itself. As has been previously raised, the Chairman should be a Parliamentarian who has had limited contact with the agencies as well as being a member of the Opposition party. The current Chairman, **Sir Malcolm Rifkind,** previously served as Foreign Secretary, and was therefore in overall charge of MI6. This is has led to questions about his impartiality.[31]

In terms of the selection process, this should be similar to the selection of Select Committee chairmen. The current system in the ISC is un-transparent and gives a disproportionate amount of power to the Executive. The proposals of **Andrew Tyrie MP** in *Neither Just nor Secure* are instructive in this case, stating that Members wishing to stand for election should submit their names to the Prime Minister for prior approval. After this stage there should be a secret ballot of MPs to confirm the final selection. [32]

When considering the resourcing of the Committee it is apparent that this requires urgent improvement. The current budget, **£1.3 million** is roughly equivalent to **0.07%** of the Single Intelligence Account Budget. This, combined with the small number of staff members, makes it very difficult for the ISC to properly carry out its investigative role.

An additional small but necessary step is allowing the ISC to hold more public evidence sessions. The Committee held its first open evidence session in November 2013, as a result of Edward Snowden's revelations. Whilst this was a welcome move it took far too long, the heads of US intelligence agencies regularly testify to Congress in public and have done so since 1975. By holding public sessions the ISC would allow members of the public to be better informed of its role and responsibilities as well as providing greater reassurance and understanding of these vital issues.

It should be noted that calls to reform the ISC are not new and are not limited to just few voices. In 2004 the Foreign Affairs Select Committee recommended that it become a full Parliamentary Committee, a move that has been backed by the former Director of Public Prosecutions, Lord Macdonald.[33,34] *The Governance of Britain*, a 2007 Green Paper, also made a series of recommendations including the introduction of open evidence sessions and a wholly transparent selection process. It is vital that these concerns are now properly

[30] Legistorm, *Staff of the House Permanent Committee on Intelligence*: http://www.legistorm.com/office/House_Permanent_Select_Committee_on_Intelligence/1538/187.html
[31] Huffington Post, *Sir Malcolm Rifkind Rejects Accusations He Is Not Fit To Scrutinise Britain's Spies*, 31st October 2013: http://www.huffingtonpost.co.uk/2013/10/31/malcolm-rifkind-isc-snowden-guardian_n_4184238.html
[32] A. Peto QC and A. Tyrie, *Neither Just nor Secure: The Justice and Security Bill* (2013) p. 91-94: http://www.cps.org.uk/files/reports/original/130123103140-neitherjustnorsecure.pdf
[33] Foreign Affairs Select Committee, *The Decision to go to War with Iraq*, 3rd July 2003, p. 5: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB80/wmd34.pdf
[34] Lord MacDonald, *The Intelligence and Security Committee should be a regular Select Committee of Parliament*: http://blogs.lse.ac.uk/politicsandpolicy/the-intelligence-and-security-committee-should-become-a-regular-select-committee-of-parliament/

dealt with.[35]

Perhaps the most damning verdict on the Committee's effectiveness can be found in the Joint Committee on Human Rights' Report: *Allegations of UK Complicity in Torture*. After recommending the ISC be made a proper Select Committee the report stated "*The recent allegations about complicity in torture should be a wake up call to Ministers that the current arrangements [of review by the ISC] are not satisfactory*."[36]

Turning to the **Commissioner system** it is clear that this too is in need of reform. The main problem is that although it ostensibly exists to ensure that the public are protected from wrongful or over-zealous intrusions into their lives, a large proportion of the public have little or no idea who the Commissioners are or what they do. This is a situation that needs to change; it should be the duty of each Commissioner to make every effort to properly communicate their work and their findings to the public.

This basic lack of transparency is something that has been recognised by both the Shadow Home Secretary and HASC. **Yvette Cooper** has commented that the system requires an "*overhaul*" in order to make it more public facing.[37] As part of their inquiry into the UK's Counter-Terrorism Strategy, **HASC** singled out the **Intelligence Services Commissioner (InSC)** and the **IoCC** for particular criticism. Their final report commented that it was "*unacceptable that there is so much confusion*" around the Commissioners' work.[38]

As **David Davis MP** has noted, part of the problem is that the Commissioners themselves are "*good people doing impossible jobs*".[39] No matter how well intentioned the efforts of the Commissioners are they simply can't be effective in their current format. Most of the Commissioners currently function on a part time basis with very small staffs.

Taking the **InSC** as an example, the difficulty of the job is clearly shown. The Commissioner, **Sir Mark Waller,** works for 120 days a year and his staff consists of a single person who functions as his "*PA*".[40] His task is to hold the Intelligence Services to account over their use of a variety of surveillance techniques. In the 2011/12 financial year, the three main agencies had a combined staff of **13,293** and a budget of "*approximately £2 billion*".[41,42] These figures show the enormity of the task faced by the Commissioner and it is

[35] Green Paper, *The Governance of Britain*, p. 32-33 (2007): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228834/7170.pdf
[36] Joint Committee on Human Rights, *Allegations of UK Complicity in Torture*, 21st July 2009, p. 26-27: http://www.publications.parliament.uk/pa/jt200809/jtselect/jtrights/152/152.pdf
[37] Y. Cooper, *The Challenges of a Digital World to our Security and Liberty*, Speech to Demos: http://press.labour.org.uk/post/78448368189/the-challenges-of-a-digital-world-to-our-security-and
[38] Home Affairs Select Committee, *Counter-Terrorism*, 30th April 2014, paragraph 166, p. 66: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf
[39] D. Davis, *Examination of Witnesses: 18th March 2014*: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf
[40] M. Waller, *Examination of Witnesses: 18th March 2014*: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf
[41] Intelligence and Security Committee, *Annual Report 2012-2013*, p. 34: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/2012-2013_ISC_AR.pdf?attachauth=ANoY7coH0ySeULUCbXSpw8N1FFLHYooyCzeYye5u1Pf4P-ayfWuXe_DL4w4BJ-EUIlwMlHgpBS-b3DWQ-YBXsyiZHMgGAtDMTwG1N_8bz6I30aZU2IxE8KP4wfZiemig4wXOBxc481eIc0zVxXlTxVMOGaLa96IyETYCWn2Cvq-PpuxqYUWEAw3KcxqYTcL41qUQJZjptwA6cDjkeiKeo-sCF1XYBdJyZN_4WZsukUH-hsi98Fur-J0%3D&attredirects=0
[42] Ibid p. 40

therefore unsurprising that he has only managed to inspect around **12%** of the warrants issued by the agencies.[43]

For a proper system of oversight the inspection figure should be at least **50%**. For this reason it is vital that the recommendations of **HASC** in this area are taken seriously. All Commissioners should be made into full time posts and their staffing and funding levels should be increased to reflect the jobs that they have to do.

One element that is almost entirely missing from UK surveillance oversight is judicial oversight. Apart from the authorization of RIPA warrants at a local government level, there is no input from judges. This is something that should be rectified.

Ideally this process would include high level judicial authorization for techniques such as:

- Interception warrants.
- Directed surveillance warrants.
- The use of Covert Human Intelligence Sources (with regard to undercover operatives).
- Intrusive surveillance.
- Certified warrants not relating to an individual.

As well as this it would be useful for low level judicial authorization to be introduced for the acquisition of communications data. As has been raised in the recent Office of Surveillance Commissioners annual report, there may be an issue with the level of technical expertise that is available in a Magistrates Court.[44] To this end we repeat the calls made in our evidence to the Joint Committee on the Draft Communications Data Bill, that a central judicial authority should be established to allow the fast and efficient resolution of requests.

The lack of judicial authorisation in the UK is something that was addressed in the 2013 report of the UN's Special Rapporteur on the promotion and protection of freedom of opinion and expression. The report warned that not including this kind of authorisation could lead to surveillance being authorised on a "*broad and indiscriminate basis, without the need for law enforcement authorities to establish the factual basis for the surveillance on a case-by-case basis*." In the recommendations it was noted that communications surveillance should only take place "*under the supervision of an independent judicial authority*."[45] [46]

One final part of the oversight system that should be discussed is the **Investigatory Powers Tribunal (IPT)**. It has failed to provide the necessary system of redress that members of the public need if they believe that they have "*been a victim of unlawful action under RIPA*."[47]

[43] M. Waller, *Examination of Witnesses: 18th March 2014*: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf

[44] Office of Surveillance Commissioners Annual Report for 2013-14 https://osc.independent.gov.uk/wp-content/uploads/2014/09/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf

[45] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (2013), p. 14: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[46] Ibid p. 21

[47] Investigatory Powers Tribunal Website: http://www.ipt-uk.com/section.aspx?pageid=1

The IPT should not hold proceedings behind closed doors. Instead, cases should be brought in an open court, subject to a closed material procedure or public interest immunity framework. This would provide a greater level of transparency on the workings of the Tribunal, whilst also allowing for secrecy where necessary. Linked to this determinations on the facts of the case should always be made public, subject to the necessary technical and operational redactions.

Currently there is no option for a successful claimant to be reimbursed for the cost that they have incurred by bringing the case. This severely limits the number of people who can bring action and leaves many completely unable to do so. If an individual is successful in their case they should be able to claim for the costs.

Linked to this is the question of informing individuals when they have been under surveillance. Currently there is no mechanism for this to take place. We therefore recommend that individuals who have been subject to surveillance under RIPA should be informed when there is no risk to an on-going investigation. Ordinarily this should happen within 12 months of the conclusion of the investigation; however allowance should be made for judicial extensions of 6 monthly increments.

The need for reform has also been recognised by figures such as Lord Dyson, the second most senior judge in the United Kingdom. He argued that there "*is no guarantee that the procedures adopted by the IPT in any particular case will satisfy the common law requirements of natural justice*."[48] The secretive role of the Tribunal has been criticised by the House of Lords Constitution Committee in a report on surveillance. The report argued that it should "*make its existence and powers more widely known to the general public*."[49]

The current system makes it virtually impossible for individuals to seek redress. There is no requirement for agencies to inform them surveillance has taken place, the process they need to follow is protracted and secretive. It is therefore beyond the average member of the public's resources to properly gain redress, this is unacceptable.

October 2014

[48] Independent, *Independent court scrutinising MI5 is located inside Home Office*, 5th March 2014: http://www.theguardian.com/politics/2014/mar/05/independence-ipt-court-mi5-mi6-home-office-secrecy-clegg-miliband

[49] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, 6th February 2009, p. 63: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf

Bingham Centre for the Rule of Law

EXECUTIVE SUMMARY

The Bingham Centre for the Rule of Law welcomes 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). The Centre's written evidence has been authored by Dr Eric Metcalfe, a Fellow of the Bingham Centre. The response draws on contributions made by experts on investigatory powers during a seminar organised by the Centre on 1 October 2014.

The Bingham Centre acknowledges that the government has a particular responsibility to protect the public from serious crime, including acts of terrorism. It therefore also accepts that in narrowly- defined and exceptional circumstances the police and intelligence services will require the power to intercept private communications, access communications data and other intrusive surveillance. In such circumstances, the need for secrecy will necessarily involve some curtailment of both the right to a fair hearing and the right to an effective remedy of those affected by the surveillance.

Nonetheless, the government does not enjoy an unlimited discretion to undertake surveillance. On the contrary, the highly exceptional nature of investigatory powers means that it is all the more important to ensure that the prevailing legal framework in respect of such powers complies with the rule of law. In particular, the law must be accessible and sufficiently certain, provide adequate protection for fundamental rights and comply with the United Kingdom's obligations under international law.

At present, the Bingham Centre has concerns about the extent to which the statutory framework governing investigatory powers falls short of these benchmarks. Accordingly, this response makes a number of recommendations that are all directed towards enhancing adherence to the rule of law and our common law constitution. It makes recommendations about the framework under the Regulation of Investigatory Powers Act 2000 (RIPA), specifically with respect to the interception of communications, the use of intercept evidence, communications data, intrusive surveillance, encryption keys, and oversight. It also makes recommendations with respect to data retention under DRIPA.

Our recommendations are:

(i) A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework.

(ii) Judicial authorisation should be required before any public body intercepts communications, accesses communications data, uses intrusive surveillance (including a covert human intelligence source), issues an encryption notice or a retention notice. The authorising judge should also have the power to direct the appointment of a special advocate to represent the interests of the subjects of

surveillance in appropriate cases.

(iii) The existing power to intercept external communications under section 8(4) RIPA should be repealed. At the very least it should be severely curtailed. All warrants and authorizations must be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity.

(iv) The statutory definition of 'intrusive' surveillance should be tightened to include *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy.

(v) The ban on the use of intercept material as evidence in criminal and civil proceedings should be lifted.

(vi) The number of public bodies able to access communications data should be curtailed.

(vii) The oversight functions currently discharged by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner should be combined into a single statutory oversight body. This body's remit should include oversight of the use of all surveillance powers by public bodies.

(viii) Any person who has been the subject of covert surveillance by a public body should be notified of that fact within a reasonable period following the conclusion of the surveillance, unless a judge is satisfied that that individual's right to an effective remedy is outweighed some specific investigative need that would otherwise be prejudiced by the disclosure.

(ix) The Investigatory Powers Tribunal should be granted the power to appoint special advocates to represent the interests of excluded parties, as well as make a declaration of incompatibility under section 4 of the Human Rights Act. Its procedural rules should also be relaxed to allow much greater disclosure to complainants who have been the subject of surveillance, in order that they may bring an effective challenge. This should include sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded. The unsuccessful party should also have the right of appeal to the Court of Appeal on a point of law.

(x) The statutory requirement that candidates for the Intelligence and Security Committee must first be nominated by the Prime Minister in order to be eligible for election should be repealed, as should the power of the Prime Minister to prevent the Committee from publishing material that it considers to be in the public interest to disclose.

INTRODUCTION

1. The Bingham Centre for the Rule of Law welcomes 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). The Centre's response is authored by Dr Eric Metcalfe (Fellow of the Bingham Centre) but also draws upon contributions from experts in a seminar organised by the Centre on 1 October 2014 and has input from senior Bingham Centre staff. The 1 October seminar programme and list of attendees is attached as an appendix.

About the Bingham Centre

2. The Bingham Centre for the Rule of Law was launched in December 2010 and is devoted to the study and promotion of the rule of law worldwide. Its focus is on understanding and promoting the rule of law; considering the challenges it faces; providing an intellectual framework within which it can operate; and fashioning the practical tools to support it. The Centre is named after Lord Bingham of Cornhill KG, the pre-eminent judge of his generation and a passionate advocate of the rule of law. It is part of the British Institute for International and Comparative Law, a registered charity based in London.

3. The Bingham Centre has a particular interest and expertise in the law governing investigatory powers. Indeed, Lord Bingham himself served as the Interception of Communications Commissioner from 1992 to 1993, although under the statutory framework that preceded the Regulation of Investigatory Powers Act 2000 (RIPA). Among the Bingham Centre's current projects is a review of the law governing the use of intercept material as evidence and on 19 September 2014 the First-Tier Tribunal (Information Rights) upheld the Centre's appeal under the Freedom of Information Act 2000 against the Home Office's refusal to disclose legal advice on this issue.[1] The Centre also held an expert seminar on the investigatory powers review on 1 October 2014 in the London offices of Macfarlanes LLP.

INVESTIGATORY POWERS AND THE RULE OF LAW

4. As a starting point, the Bingham Centre acknowledges that the government has a particular responsibility to protect the public from serious crime, including acts of terrorism.[2] Although this submission does not address "current and future threats to the United Kingdom" (s7(2)(a)), it nonetheless proceeds on the assumption that the United Kingdom will continue to face grave threats to its national security and the safety of its public.

5. On the same basis, the Bingham Centre accepts that the police and intelligence services will - in certain, narrowly-defined and exceptional circumstances - continue to require the power to intercept private communications, access communications data, together with other forms of intrusive surveillance such as the use of covert sources

[1] *Bingham Centre for the Rule of Law v Information Commissioner* [2014] UKFTT 2014/0097 (GRC).
[2] See e.g. the judgment of the European Court of Human Rights in *Öneryildiz v Turkey* (2005) 41 EHRR 20 in which the Grand Chamber held that the right to life under Article 2 ECHR requires governments to "put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life" (para 89).

and the power to demand encryption keys. As the European Court of Human Rights held in *Klass v Germany,* "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[3]

6. The Bingham Centre also recognises that the very effectiveness of covert surveillance depends upon it remaining secret while it is being carried out, and that this secrecy necessarily involves some curtailment of both the right to a fair hearing and the right to an effective remedy of those affected by the surveillance.[4] The necessity of this interference, however, does not mean that the government enjoys an "unlimited discretion" to undertake surveillance.[5] On the contrary, the highly exceptional nature of such powers means that it is all the more important to ensure that the legal framework for investigatory powers complies with the rule of law, including in particular that it must be accessible and sufficiently certain, provide adequate protection for fundamental rights and comply with the United Kingdom's obligations under international law.[6] In our view, these are the benchmarks against which the adequacy of the existing law should be assessed.

THE EXISTING LAW GOVERNING INVESTIGATORY POWERS

7. Although s7(1) DRIPA requires the Home Secretary to appoint the Independent Reviewer "to review the operation and regulation of investigatory powers", the term "investigatory powers" is itself nowhere defined, either in DRIPA, RIPA or elsewhere. On its face, it is an extremely broad term, suggesting any statutory power that may be used by a public body for the purposes of investigation. While in practice it is generally understood as synonymous with "surveillance powers", this only begs the question of how "surveillance" is defined. Even taking a narrow definition of "surveillance", e.g. the *covert* use of statutory powers to collect *private* information about an individual, it is apparent that this would include a great many statutory powers outside either RIPA or DRIPA. For instance:

   (a) Section 94(1) of the Telecommunications Act 1984 allows the Secretary of State to give directions to telecommunications service providers "in the interests of national security or relations with the government of a country or territory outside the United Kingdom";

---

[3] *Klass v Germany* (1980) 2 EHRR 214 at para 48.

[4] See e.g. *Klass* at para 55: "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge." See also Lord Neuberger's reference in *In re McE* [2009] UKHL 15 to certain "inherent paradoxical problems" involved in surveillance, one of which is that the authorities "cannot warn the parties in advance that interception or listening in will or will not occur, as to do so would defeat the whole point of the exercise" (para 111).

[5] C.f. *Klass* at para 49: the latitude afforded to domestic legislatures "does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

[6] See e.g. Tom Bingham, *The Rule of Law* (Penguin, 2010), Part 2, pp37-129.

(b) Part III of the Police Act 1997 provides a framework for authorising interference by police with private property, including the use of surveillance devices;

(c) A number of statutes grant public bodies power to access communications data in certain circumstances, including the Police and Criminal Evidence Act 1984, the Social Security Fraud Act 2001, the Charities Act 1993, the Criminal Justice Act 1987, the Environmental Protection Act 1990, the Financial Services and Markets Act 2000 and the Health and Safety at Work Act 1974;[7]

(d) Section 1(5)(c) RIPA similarly provides for the power of public bodies to intercept stored communications without a warrant by way of "*any statutory power* that is exercised ... for the purpose of obtaining information or of taking possession of any document or other property";

(e) Although the Data Retention (EC Directive) Regulations 2009 (SI 2009/859) have now been superseded by Part 1 of DRIPA, the power of the Secretary of State to provide codes of practice for the retention of communications data continues to be set out in Part 11 of the Anti-Terrorism Crime and Security Act 2001.

8. For practical reasons, this submission has focused primarily on those powers contained in RIPA and DRIPA. In our view, however, it is clear that there is a broader need for a coherent and, ideally, comprehensive statutory framework governing the use of covert surveillance powers in general.[8]

Interception of communications

Authorisation

9. The Bingham Centre does not doubt the diligence and conscientiousness of the Secretaries of State in issuing interception warrants nor does it have cause to dispute the candour and integrity

[7] Section 1(6) DRIPA now provides that a public telecommunications operator who retains relevant data under Part 1 of DRIPA must not disclose it except in accordance with an authorisation under Chapter 2 of Part 1 of RIPA, "a court order or other judicial authorisation or warrant" or as provided by regulations made under s1(3) DRIPA.

[8] See e.g. the Report of the Newton Committee of Privy Counsellors on the Anti-Terrorism Crime and Security Act 2001 (HC100, December 2003) at para 406: "we recognise that the need to retain communications data for terrorism and other serious crimes creates the potential for other use or abuse of that data. The protection provided by the Regulation of Investigatory Powers Act is a step in the right direction where it applies, but a coherent legislative framework governing both retention of, and access to, communications data seems to be the only way of providing a comprehensive solution to this issue"; and Lord MacDonald QC, *Review of Counter-Terrorism and Security Powers* (Cm 8003, January 2011) at p7: "although RIPA is the principle legal framework under which communications data may be acquired, there is a wealth of other statutes under which local authorities may also acquire such data. The Review has found that these were mostly not designed with the acquisition of communications data in mind, so that they contain significantly fewer safeguards. This is a very unsatisfactory situation and it needs to be addressed with real urgency if public confidence is to be maintained".

and of those applying for such warrants.[9] We nonetheless consider that it is constitutionally inappropriate for the Secretary of State to have the final say in issuing interception warrants. In their evidence before the Intelligence and Security Committee, the Home Secretary and the Foreign Secretary both stressed the need for democratic accountability in issuing interception warrants, so that government ministers remained answerable for the warrants they issued and could be removed by way of the ballot box if necessary.[10] Yet it is very difficult to see how this could ever be the case. For a start, s17 RIPA prohibits any evidence being adduced in any court or tribunal that would even "tend ... to suggest" that an interception warrant has been made.[11] Secondly, s19 RIPA provides that it is a criminal offence for any person "holding office under the Crown", any member of staff of an intercepting agency or communications service provider, among others, to disclose the existence of an interception warrant unless authorised to do so for certain limited purposes, none of which appear to entail disclosure to Parliament or the public at large.[12]

10. Indeed, in the nearly thirty years since the power to intercept communications has been put on a statutory footing, we are not aware of a single instance in which it was revealed that a government minister signed a particular interception warrant, still less that any minister has ever appeared before Parliament or any court or tribunal or inquiry to account for having done so. In our view, this is because the same secrecy that rightly attaches to the interception of communications by police and intelligence services also prevents meaningful democratic accountability for the Secretary of State's decision to authorise such interception in particular cases.

---

[9] Having said that, we note that concerns have been raised at times; see the remarks of Lord Neuberger in *R(Binyam Mohamed) v Secretary of State for the Foreign and Commonwealth Affairs* [2010] EWCA Civ 65 at para 168, concerning the preparation of public interest immunity certificates: "as the evidence showed, some Security Services officials appear to have a dubious record relating to actual involvement, and frankness about any such involvement, with the mistreatment of Mr Mohamed when he was held at the behest of US officials. I have in mind in particular witness B, but the evidence in this case suggests that it is likely that there were others. The good faith of the Foreign Secretary is not in question, but he prepared the certificates partly, possibly largely, on the basis of information and advice provided by Security Services personnel. Regrettably, but inevitably, this must raise the question whether any statement in the certificates on an issue concerning the mistreatment of Mr Mohamed can be relied on, especially when the issue is whether contemporaneous communications to the Security Services about such mistreatment should be revealed publicly. Not only is there some reason for distrusting such a statement, given that it is based on Security Services' advice and information, because of previous, albeit general, assurances in 2005, but also the Security Services have an interest in the suppression of such information."

[10] "Theresa May's evidence to the intelligence and security committee", by Andrew Sparrow, *The Guardian,* 16 October 2014; "Ministers should assess UK surveillance warrants, says Philip Hammond" by Julian Borger, *The Guardian*, 23 October 2014: "'Perhaps it is a feature of the times that we live in, but I'm sure I can speak for all my colleagues who sign warrants that we all have, in the back of our minds, that at some point in the future we will – not might be, but will – be appearing before some inquiry or tribunal or court to account for the decisions we've made', Hammond said."

[11] Section 18 RIPA provides for certain exceptions to this, yet it is notable that almost all of these relate to courts and tribunals with the power to hold closed proceedings and which are generally under a duty to prevent the disclosure of information contrary to the public interest.

[12] Although s19(9) grants the Interception of Communications Commissioner the power to authorise disclosure, he reports in the first instance to the Prime Minister (s58(4)) who in turn may exclude material contained in the Commissioner's report from being laid before Parliament if he considers that it would be contrary to the public interest for reasons of national security, et al.

11. Moreover, it is generally the case that the Secretary of State who considers an application for a warrant from an intercepting agency is the same person who is accountable to Parliament for its performance, e.g. the Foreign Secretary in the case of MI6 and GCHQ; the Home Secretary in the case of the National Crime Agency, MI5 and the Metropolitan Police; and so forth.[13] There is, therefore, an inevitable risk that, when considering whether to grant an interception warrant, the Secretary of State may give undue weight to broader political considerations at the expense of the fundamental rights of those affected by the surveillance. This risk is especially serious in cases involving the threat of terrorism, and where the rights in question are those of unpopular minorities.[14] In a 2009 case involving directed surveillance of privileged conversations between lawyers and persons in custody, for instance, Lord Neuberger expressed concern at the possibility "that the Government has been knowingly sanctioning illegal surveillance for more than a year".[15] Despite this adverse comment, however, there is no indication that the government faced any public outcry or parliamentary censure as a result of this failing.

12. Even where democratic accountability of surveillance decisions *is* possible (i.e. because authorisations for directed surveillance, unlike interception warrants, may sometimes be disclosed), as the case of *In re McE* shows, the rights of unpopular minorities may be vulnerable where the decision to authorise surveillance is left to the executive. As the ECtHR held in *Klass*:[16]

> *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 a proper procedure.*

[13] Save in the case of Scottish warrants for serious crime, s7 RIPA refers only to the power of the Secretary of State to issue warrants and therefore it is exercisable by any of the Secretaries of State: see Schedule 1 of the Interpretation Act 1978. The practice, however, is as outlined above.

[14] See e.g. the judgment of Lord Dyson in *Walumba Lumba v Secretary of State for the Home Department* [2011] UKSC 12 concerning a secret policy operated by the Home Office between 2006 and 2008 concerning the blanket detention of foreign prisoners: "It is material that there is no suggestion that officials acted for ulterior motives or out of malice towards the appellants. Nevertheless, there was a deliberate decision taken at the highest level to conceal the policy that was being applied and to apply a policy which, to put it at its lowest, the Secretary of State and her senior officials knew was vulnerable to legal challenge. For political reasons, it was convenient to take a risk as to the lawfulness of the policy that was being applied and blame the courts if the policy was declared to be unlawful" (para 166).

[15] *In re McE* [2009] UKHL 15 at para 119. At the time of writing, we note also the revelations regarding surveillance of privileged lawyer-client conversations: see *Belhadj & others v Security Service & others*, Case IPT/13/132-9/H, 'Respondents' revised response to claimants' request for further information' 29 October 2014. Documents available in O Bowcott, 'UK intelligence officers spying on lawyers in sensitive security cases', 7 Nov 2014 http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client- abdel-hakim-belhaj-mi5-mi6-gchq.

[16] Para 55. See also e.g. para 56: "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge". The requirement for judicial authorisation is even more explicit in cases involving the seizure of journalistic material under Article 10 ECHR: see e.g. *Sanoma Uitgebers BV and others v Netherlands* (2010) 51 EHRR 31.

13. The Court in *Klass* did not exclude the possibility that effective control could also be exercised by a non-judicial body, so long as it could be shown that it was "independent of the authorities carrying out the surveillance" - i.e. "enjoying sufficient independence to give an objective ruling" - well as "vested with sufficient powers and competence to exercise an effective and continuous control".[17] In our view, however, it cannot be said that the Secretaries of State are sufficiently independent of the agencies that apply to them for interception warrants; this is because they are accountable to Parliament for the performance of those same agencies.[18] It is *this* aspect of democratic accountability which, in our view, makes government ministers constitutionally ill-suited to grant interception warrants. It is, of course, true that in *Kennedy v United Kingdom,* the Strasbourg Court considered that the Interception of Communications Commissioner and the Investigatory Powers Tribunal provided sufficient judicial control of interception warrants issued by the Secretary of State.[19] For reasons set out in detail below,[20] however, we consider that neither body can properly be said to "exercise an effective and continuous control" over interceptions, and that the ECtHR in *Kennedy* therefore misapprehended the true position under RIPA.

14. Other arguments against judicial authorisation of interception include that it would undermine operational effectiveness,[21] that it would be more resource-intensive than the current model; that it would prevent or inhibit continuing or "downstream" oversight of how interception material is retained and shared. However, these arguments tend to overlook how RIPA *already* provides for judicial authorisation of certain surveillance powers:
    (a) authorisations for police to use intrusive surveillance under Part II must first be approved under s36 RIPA by a Surveillance Commissioner (a person who holds or has held high judicial office under s91(2) of the Police Act 1997);

[17] Ibid, para 56.

[18] See e.g. *Kopps v Switzerland* [1999] 27 EHRR 91 at para 74: "It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence".

[19] (2011) 52 EHRR 4 at paras 166-167.

[20] Paras 40-53.

[21] See e.g. the evidence of the then-Interception of Communications Commissioner Sir Swinton Thomas to the Joint Committee on Human Rights: "From a practical point of view, which I suppose is what I am more concerned with, I think it is a very bad idea to put [interception decisions] in the hands of a judge. As things are at the moment, if you know that a bomb has been taken on a train in Leeds and is on its way to King's Cross and you need information, in a matter of minutes you can get a warrant to intercept the communications of that suspected terrorist. Likewise with a serious crime, if a very large consignment of class A drugs has arrived at Dover and is on its way up to Manchester, the Secretary of State is always on duty, 24 hours a day. It is very often absolutely vital that you act with as much speed as you possibly can. That is what currently happens. You can get a warrant or a modification, which is equally important, straight away. Going to a judge would not permit that degree of elasticity. If it is done by a judge, the other side must have the right to be heard and you will not be able to acquire a judicial hearing at the sort of speed that papers can be put in front of the Secretary of State" (12 March 2007, Q26). However, as the then-Director of Public Prosecutions Sir Ken Macdonald QC explained in the same evidence session, there is no reason why judicial authorisation for interception should not be done on an *ex parte* basis (see Q27) and, as Lord Lloyd of Berwick pointed out, there would be no difficulty in getting judicial authorisation "almost as quickly" as with the Secretary of State (Q28).

(b) authorisations for local authorities to access to communications data, use directed surveillance, or covert human intelligence sources must first be approved by a magistrate under ss23A-D RIPA (as amended by ss37-38 of the Protection of Freedoms Act 2012); and

(c) permission to make an encryption notice under Part III must be given by a Circuit judge under paragraph 1(1) of Schedule 2 RIPA.[22]

15. Of these, we consider that the work of the Surveillance Commissioners in approving the use of intrusive surveillance by police provides a useful model for judicial authorisation of interception warrants under RIPA for the following reasons:

(i) it is well-known that intrusive surveillance may enable police to access the contents of private communications almost as readily as interception (e.g. recording a telephone conversation by way of a covert listening device or viewing a computer screen by way of a hidden camera);[23]

(ii) the Surveillance Commissioners are already obliged to consider the likelihood that the use of intrusive surveillance may result in the acquisition of legally privileged material (as well as the likelihood of obtaining "confidential information" under the Police Act 1997, including not only privileged material but also confidential journalistic material, personal information, or communications with an MP on constituency matters);[24]

(iii) s36(2) RIPA provides for police to use intrusive surveillance without judicial approval in cases of urgency, subject to subsequent review by a Surveillance Commissioner who has the power to quash or cancel such authorisations under s37(2) or (3). (We note, moreover, that this is consistent with the procedures in most countries which require judicial authorisation for interception, in that they allow for emergency self-authorisation by police subject to judicial confirmation within 24 or 48 hours);[25]

(iv) in addition to approving the use of intrusive surveillance by police, the Surveillance Commissioners also provide "downstream" oversight by way of their role in reviewing the renewal of authorisations as well as by way of the annual report of

[22] Save where the police or intelligence services have obtained the encrypted material by way of a warrant made by the Secretary of State: see paragraph 2 of Schedule 2 RIPA.

[23] See e.g. *R v Allsop and others* [2005] EWCA Crim 703; *R v E* [2004] EWCA Crim 1243; *R v Smart and another* [2002] EWCA Crim 772.

[24] In her evidence to the Intelligence and Security Committee in October 2014, the Home Secretary suggested that a key difference between judicial authorisation of search warrants and that of interception warrants was that a search takes place in public whereas surveillance involves a different kind of intrusion. In our view, however, the different nature of the intrusion only makes judicial authorisation *more* necessary.
More to the point, intrusive surveillance by the police under Part II RIPA also involves considerable secrecy, yet it is not suggested that judicial authorisation in these cases is somehow less appropriate.

[25] See e.g. 18 US Code § 2518(7), enabling interception without a judge's order where there is immediate danger of death or serious physical injury, or "conspiratorial activities" which either threaten national security or are characteristic of organized crime, so long as an application is made to a judge within 48 hours.

the Chief Commissioner under s62 RIPA. Again, this is consistent with the procedure of other jurisdictions which require judicial authorisation;[26]

(v) the Surveillance Commissioners have each held high judicial office, which means that they are each former Court of Appeal or High Court judges or their Scottish equivalent.

16. We do not suggest that it is the Surveillance Commissioners themselves who should necessarily assume responsibility for making interception warrants: in our view, the same function could in principle also be carried out by any High Court judge (see e.g. their expertise in cases involving terrorist asset-freezing, TPIMs and deportation on grounds of national security) or even the specialist district court judges who preside over cases involving extradition or terrorism. If judicial supervision is possible in these areas involving highly sensitive matters of national security and close scrutiny of the activities of the intelligence services, then it should also be possible in the case of interception of communications. In any event, the role of the Surveillance Commissioners shows not only how judicial authorisation of surveillance powers *may* work in practice, but also that it *has* worked for nearly fifteen years under Part II of RIPA.[27]

17. For the avoidance of doubt, we do not recommend that the judge's task be confined to deciding whether or not to *approve* an authorisation – rather, the relevant agency should apply for an interception warrant in the same manner as a search warrant, i.e. it is for the judge himself or herself to decide whether the surveillance sought is necessary and proportionate, rather than simply reviewing whether the applicant's assessment of necessity and proportionality was reasonable. We also recommend that the judge should have the power to direct the appointment of a special advocate in appropriate cases (e.g. where the application is particularly complex) in order to test the application in a closed hearing, just as a judge may currently do in cases involving public interest immunity[28] and is routinely the case in applications for surveillance in Queensland, Australia.[29]

Bulk interception of 'external' communications under s8(4)

18. At the time of writing, the legality of warrants for the bulk interception of external communications under s8(4) RIPA is the subject of several legal challenges, before both

[26] See e.g. 18 US Code § 2518(6), under which an interception order "may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception".

[27] Moreover, if it is correct that the Home Secretary spends a "significant part of her day dealing with intercept and surveillance warrants",(see "Theresa May defends culture of secrecy over mass snooping" by Alan Travis, The Guardian, 16 October 2014) then it is apparent that an additional benefit of judicial authorisation is that it would enable each of the relevant Secretaries of State to devote more time to those duties to which they are constitutionally better-suited to discharge.

[28] See *R v H* [2004] UKHL 3 at para 36.

[29] See the role of the Public Interest Monitor under s326(b) of the Crime and Misconduct Act 2001 (Qld) as set out in JUSTICE, *Secret Evidence* (June 2009) at paras 333-337.

the Investigatory Powers Tribunal[30] and the European Court of Human Rights.[31] In outline, the key issues are as follows:

(a) unlike a warrant issued under s8(1), there is no requirement for a warrant under s8(4) to be targeted at the communications of either a particular person or a specific premises. As the Investigatory Powers Tribunal noted in *British Irish Rights Watch and others v Security Service and others*, a warrant under s8(4) may in principle result in "the interception of all communications between the United Kingdom and an identified city or country".[32] The only constraint is what the Secretary of State considers to be necessary in the interests of national security, the detection or prevention of serious crime, safeguarding the economic well-being of the United Kingdom,[33] or for the purposes of giving effect to an international mutual legal assistance agreement (s5(3) RIPA);

(b) although a warrant under s8(4) only authorises the interception of "external" communications (defined by s20 as those either sent or received outside the British Islands), s5(6) RIPA further authorises the interception of any such communications not identified by the warrant as is necessary in order to intercept the external communications in question. As Lord Bassam told Parliament in 2000, "it is just not possible to ensure that only external communications are intercepted" and "there is no way of filtering ... out [internal] communications without intercepting the whole link".[34] In practical terms, therefore, the interception of external communications is liable to involve the interception of an unknown number of internal communications as well;

(c) although Parliament was told in 2000 that email sent and received within the UK would not fall within the definition of "external communications" under s20, even if it was routed outside the UK in transit,[35] it remains unclear how this definition would apply to such activities as an inquiry made of a search engine or a post to a friend's page using social media. It was not until 16 May 2014 that a senior Home Office official revealed in a witness statement that the intelligence services considered that search engine inquiries and posts to social media platforms were "external communications" for the purposes of s8(4) RIPA, so long as the relevant server was outside the British Islands, notwithstanding that the only persons involved in the communication were within the UK at all material times;[36]

---

[30] See *Liberty, the ACLU and others v GCHQ and others* (IPT/13/77H, IPT/13/168-173/H); *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (IPT/13/92/CH); and *Amnesty International v The Security Service and others* (IPT/13/194/CH).

[31] See *Big Brother Watch and others v United Kingdom* (no 58170/13, lodged 4 September 2013).

[32] IPT/01/77, 9 December 2004 at para 9.

[33] This ground has now been narrowed by s3 DRIPA to only those economic interests that are "also relevant to the interests of national security". In addition, s5(5) RIPA has always provided that a warrant cannot be necessary for the purposes of safeguarding economic interests unless the information in question relates "to the acts or intentions of persons outside the British Islands"

[34] Hansard, HL debates, 12 July 2000, col 323.

[35] See the speech of Lord Bassam, ibid and para 5.1 of the Interception of Communications Code of Practice, issued in July 2002 under s71 RIPA.

[36] See witness statement of Charles Farr dated 16 May 2014 at paras 132-138.

(d) the primary safeguard to prevent internal communications collected under s8(4) warrants being "read, looked at or listened to" by the intelligence services is that set out under s16(2), which prohibits officials from selecting material for inspection by reference to a factor which is "referable to an individual who is known to be for the time being in the British Islands", where one of the purposes of the search is to identify "material contained in communications sent by him or intended for him". There is nothing in s16 or elsewhere in RIPA, however, to prevent a person's internal communications being searched by reference to *other* factors which may nonetheless lead to disclosure of his or her sensitive personal information, e.g. religious beliefs, medical status, sexual orientation or political opinions;

(e) on the same basis, there is nothing under s16 or elsewhere in RIPA to prevent the *data* related to internal communications intercepted under s8(4) - e.g. traffic data, subscriber data and service use data - being collected, retained and used by the intelligence services for whatever purpose they consider to be necessary for the purposes of national security, etc under s5(3). To the extent that there is any internal guidance that further restricts how internal communications and related data may be used, the intelligence services have refused to disclose this on the grounds that it would be prejudicial to national security.

19. In the Bingham Centre's view, the current framework governing the bulk interception of communications and related data under s8(4) raises a number of concerns.[37] First, the relevant provisions - especially the definition of "external communication" under s20 - appear to us to lack sufficient clarity and certainty to comply with the fundamental requirements of the rule of law.[38] Secondly, we doubt whether the location from which a particular communication was sent or received (i.e. within or without the British Islands) provides a sufficient basis on which to distinguish between the narrow and targeted requirements of warrants under s8(1) with the virtually unrestrained breadth of warrants under s8(4). Thirdly, the practice of bulk interception in which potentially millions of internal communications may be intercepted for the sake of obtaining a particular external communication - seems to us to be fundamentally at odds with the very concept of proportionality itself. In our view, all warrants and authorisations must

[37] For reasons of space, we are unable to address an equally pressing issue which is the extent to which the intelligence services may *receive* communications data and the contents of communications collected by foreign intelligence agencies.

[38] C.f.. *Liberty and others v United Kingdom* (2009) 48 EHRR 1 at para 69, in which the ECtHR held that the relevant provisions of the Interception of Communications Act 1984 breached Article 8 ECHR because, inter alia, they did not "indicate with sufficient clarity ... the scope or manner of the very wide discretion conferred on the State to intercept and examine external communications ... In particular it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material"; see also *Weber and Saravia v Germany* (2008) 46 EHRR SE5 at para 94: the law governing interception must "indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".

be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity (which would, of necessity, include terrorist offences).

20. Nor is the scale of the apparent interference with the right to privacy mitigated by the fact that relatively few of the communications intercepted by the intelligence services under a s8(4) warrant may be "read, looked at or listened to" under s16(2). In this context, we note the recent judgment of the CJEU in *Digital Rights Ireland*, in which the Grand Chamber held that the blanket retention of customers' communications data for up to 2 years under the 2006 Data Retention Directive entailed "an interference with the fundamental rights of practically the entire European population" contrary to the rights to privacy and data protection under Articles 7 and 8 of the EU Charter of Fundamental Rights because it did "not require any relationship between the data whose retention is provided for and a threat to public security".[39]

21. For these reasons, we recommend that the current power to intercept external communications under s8(4) be repealed. At the very least it should be severely curtailed. We note that there is no statutory restriction against using s8(1) warrants in respect of so-called "external" communications. We see no reason, therefore, why targeted warrants should not be used in respect of external communications on the same basis that they are used within the UK.

Intercept as evidence

22. Section 17(1)(a) RIPA prohibits the use of intercept obtained under warrant as evidence in either criminal or civil proceedings.[40] In January 2008, a review committee of Privy Counsellors reported its conclusion that "intercept as evidence should be introduced", subject to certain operational tests that would have to be met.[41] In December 2009, the Home Secretary reported to Parliament that it had been unable to produce a viable model that met the legal requirements identified by the Privy Council.[42] The Home Secretary nonetheless stated that the Home Office's implementation team would continue to work to "identify a way forward".[43] As recently as June 2013, a Home Office minister told Parliament that the government was continuing to review the use of intercept as evidence, "under the guidance of the cross-party group of Privy Counsellors" and that it would "report back to the House in due course".[44] As of yet, there has been no subsequent report.

23. In our view, intercept evidence is one of the most compelling and probative forms of evidence available.[45] It is widely used in other common jurisdictions with similar criminal

[39] *Digital Rights Ireland v Minister for Communications and others* (2014) ECLI:EU:C:2014:238 at paras 56 and 59.
[40] Notably, evidence obtained by way of interception without a warrant under ss3 or 4 RIPA (e.g. interceptions in prisons, etc) *are* admissible.
[41] Cm 7324, at para 204.
[42] Cm 7760 at paras 23-25.
[43] Ibid, para 25.
[44] 6 June 2013, col 1229W.
[45] As Lord Lloyd of Berwick told Parliament during the debates on what became s17: "We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting

and civil proceedings as our own,[46] including some with more onerous requirements governing the disclosure of relevant unused material.[47] And, as Lord Bingham noted in 2004, there is nothing in the ECHR that prohibits the use of intercept as evidence.[48] On the other hand, the lack of provision for intercept evidence has not only made it more difficult to prosecute terrorism offences, but increased resort to exceptional measures such as TPIMs.[49] We therefore consider it essential that any reform of the legal framework of investigatory powers in the UK must address the issue of intercept evidence.

Communications data

The changing nature of communications data

24. The lower level of protection accorded to communications data under Chapter 2 of Part 1 of RIPA reflects the longstanding view that the content of any given communication is necessarily more sensitive than the data which relates to it. In the

---

terrorist offenders because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so" (Hansard, HL Debates 19 June 2000, col 109-110); see also the views of the Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning*, HL157/HC 394, 16 July 2007 at para 126: "We are satisfied that the evidence of the DPP and the former Attorney General puts the matter beyond doubt: that the ability to use intercept as evidence would be of enormous benefit in bringing prosecutions against terrorists in circumstances where prosecutions cannot currently be brought, and that the current prohibition is the single biggest obstacle to bringing more prosecutions for terrorism. We recommend that this be taken as the premise of the forthcoming review by the Privy Council. The difficult question is not whether the current ban on the evidential use of intercept should be relaxed, but how to overcome the practical obstacles to such a relaxation".

[46] See e.g. *Intercept Evidence: Lifting the Ban* (JUSTICE, October 2007).

[47] See e.g. "The Unique Challenges of Terrorism Prosecutions" (Ch 7) vol 4 at p267), *Air India Flight 192: A Canadian Tragedy* (June 2010): "In general, disclosure obligations in both the United States and the United Kingdom are less broad than in Canada. Both the United States and the United Kingdom attempt to flesh- out disclosure requirements in statutes and other rules while, as discussed above, Canada relies on a case- by-case adjudication under the Charter. Both the decreased breadth and increased certainty of disclosure requirements in the United States and the United Kingdom may make it less necessary for prosecutors to claim national security confidentiality over material that may be relevant to a case, but which does not significantly weaken the prosecution's case or strengthen the accused's case."

[48] *Attorney General's Reference No 5 of* 2002 [2004] UKHL 40 at para 14: "the United Kingdom practice has been to exclude the product of warranted interception from the public domain and thus to preclude its use as evidence. But this has been a policy choice, not a requirement compelled by the Convention, and other countries have made a different policy choice. Article 8(2) of the European Convention permits necessary and proportionate interference with the right guaranteed in Article 8(1) if in accordance with the law and if in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. Save where necessary to preserve the security of warranted interception, there is no reason why it should have been sought to exclude the product of any lawful interception where relevant as evidence in any case whether civil or criminal".

[49] See e.g. Home Office Minister Lord Rooker, Hansard, HL Debates, 27 November 2001, col 146: "If we could prosecute on the basis of the available evidence in open court, we would do so. *There are circumstances in which we simply cannot do that because we do not use intercept evidence in our courts*".

1984 case of Malone v United Kingdom,[50] for instance, the British government had argued that the practice of 'metering' (which involved a meter check printer being attached covertly to a telephone line to record "the numbers dialled on a particular telephone and the time and duration of each call")[51] did not entail any interference with the applicant's rights under Article 8 ECHR. Although this argument was rejected by the ECtHR on the basis that the relevant data was "an integral element in the communication", it accepted that the collection of data was nonetheless to be distinguished from the interception of content.[52]

25. It is obvious, however, that there has been a fundamental shift in the nature of communications technology over the past three decades. Not only is there increasing convergence of communications *networks* (e.g. voice and data being carried on the same infrastructure) but also a convergence of *functions*, so that most individuals now carry at least one or more devices which are each capable of communicating in a number of different ways, e.g. a person who uses his or her mobile phone to make calls, send texts and emails, post on social media and browse websites on the Internet.

26. In addition to the fact that most of our private communications are now made via the Internet, it is also apparent that there has been a vast increase in the amount of communications data that is generated by each person, which is then automatically collected and stored by a wide range of communications service providers and accessible to public authorities under RIPA. It is apparent that the analysis of such data – including not only numbers dialled and the time and duration of a call but also geo-location data and the IP addresses of websites visited – can readily disclose details of a person's relationships with others as well as various patterns of behaviour capable of revealing broad range of sensitive information about that individual, including their ethnic origin, their political opinions or religious beliefs, their physical or mental health, and/or their sexual orientation.[53]

27. In our view, it is clear that there is very little meaningful comparison between the quality of information available from the Post Office's metering of a single landline in the early 1980s and that available from an ordinary mobile phone more than three decades later.

---

[50] (1984) 7 EHRR 14.
[51] Ibid, para 83.
[52] Para 84.
[53] For example, a study by the Center for Internet and Society at Stanford Law School analysed the communications data gathered from 546 mobile phone users ("MetaPhone: The Sensitivity of Telephone Metadata" by Patrick Mutchler and Jonathan Mayer, 12 March 2014). In the first instance, it noted that, in certain cases, the simple fact that a number was called was itself highly sensitive in nature: "Participants had calls with Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more". The study went on to find "a number of patterns that were highly indicative of sensitive activities or traits", for example:
"Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis" and "Participant E had a long, early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after".

The idea that intercepting the content of a person's communications is always more intrusive than accessing their communications data is simply no longer sustainable. The interception of the content of any particular telephone call by an individual may reveal very little about that person's religious beliefs, their medical information or their sexual orientation. Access to and analysis of the communications data from the same person's mobile phone may, by contrast, readily disclose a wealth of highly sensitive information about that person, all without a single word of their communications being read, looked at or listened to by anyone else. By the same token, it is equally true that access to communications data may also disclose information subject to legal professional privilege or the identity of a journalist's source. We are concerned, therefore, by recent revelations that the Metropolitan police may have been using authorisations under Chapter 2 to access communications data as a means of avoiding the requirements of the Police and Criminal Evidence Act 1984 in respect of journalistic material.[54]

Authorisation

28. Given the obvious sensitivity of communications data, it is clear that existing procedures for authorising access to such data are inadequate. In the first instance, Chapter 2 of Part 1 of RIPA provides that when a public body seeks access to communications data, the person responsible for authorising the request is, in almost every case, a senior member of the same agency. Even if senior officials scrutinize applications for communications data with great care, it is plain that they are not independent of the agency carrying out the surveillance and are therefore institutionally incapable of the objectivity needed to give an impartial decision on the merits of the application.

29. In this respect, we note that Protection of Freedoms Act 2012 introduced a requirement for prior judicial authorisation of communications data requests by local authorities, together with a power for the Secretary of State to extend this requirement to other public bodies by way of an order. While this might at first glance appear to provide an appropriate way forward, we note that serious concerns have been expressed that many magistrates do not have sufficient training or expertise to provide the necessary degree of supervision.[55] We therefore recommend that authorisation for access to communications data should be placed on the same footing as the interception of communications: i.e. ideally authorised High Court judges or their equivalent. Similarly, in cases of urgency, the police and intelligence services should have the power to self-

[54] See, for example, 'A Travis, 'Police told to reveal the use of surveillance powers to identify journalists' sources', *The Guardian*, 6 Oct 2014, http://www.theguardian.com/uk-news/2014/oct/06/police-ordered- reveal-ripa-powers-identify-journalists-sources. We welcome the government's undertaking to reform the law: P Wintour, 'British police's use of Ripa powers to snoop on journalists to be reined in' *The Observer*, 12 Oct 2014, http://www.theguardian.com/world/2014/oct/12/police-ripa-powers-journalists-surveillance.

[55] See e.g. the 2014 report of the Chief Surveillance Commissioner at para 3.10: "What has become clear is that the knowledge and understanding of RIPA among magistrates and their staff varies widely. Adequate training of magistrates is a matter for others, but I highlight the need. The public is not well served if, through lack of experience or training, magistrates are not equipped effectively to exercise the oversight responsibility which the legislation requires. I am aware, for example, of one magistrate having granted an approval for activity retrospectively, and another having signed a formal notice despite it having been erroneously completed by the applicant with details of a different case altogether."

authorise access to communications data so long as it is subject to judicial confirmation within 48 hours.

30. A separate concern is that, unlike interception warrants under s8(1), there is no requirement that a request for access to communications data be targeted against a particular individual. We therefore recommend that this requirement be introduced to ensure that the power to access communications data is not exercised disproportionately.

31. More generally, we recommend that both the number of statutory powers to access communications data and the number of public bodies able to wield those powers should be severely curtailed. In the latter case, we recommend that the power to access such data should be restricted to the police, the intelligence services and the limited number of other public bodies with a responsibility to investigate serious criminal activity.[56] As regards the former, we note that the current government has already committed itself to ensuring that "RIPA is the only mechanism by which communications data can be acquired"[57] and we further note the requirement in s1(6) DRIPA prohibiting disclosure of communications data retained by a public telecommunications operator pursuant to a retention notice other than by way of Chapter 2 RIPA or "a court order or other judicial authorisation or warrant" or under regulations made by the Secretary of State. Although this is a welcome move, we note that it does not prevent access to communications data held by *other* communications service providers otherwise than pursuant to a retention notice, nor has the Secretary of State published any regulations in draft.

Intrusive surveillance, directed surveillance and covert sources

32. The distinction under Part 2 RIPA between 'intrusive' and 'directed' surveillance is meant in principle to ensure that any surveillance that is likely to involve a serious interference with a person's privacy (i.e. intrusive) requires a much higher level of authorisation than those which do not (i.e. directed). However, as the Code of Practice itself notes, the statutory definition of 'intrusive' "relates to the *location* of the surveillance [i.e. within a person's home or vehicle] and *not* any other consideration of the nature of the information that is expected to be obtained". It is therefore not necessary, the Code continues, "to consider whether or not intrusive surveillance is likely to result in the obtaining of private information".[58] Part 3 of the Police Act 1997, by contrast, requires judicial authorisation whenever property interference is likely to result in "the acquisition of knowledge of matters subject to legal privilege, confidential personal information or confidential journalistic information".[59]

---

[56] C.f. the 2009 recommendation of the House of Lords Constitution Committee that "such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years" (*Surveillance, Citizens and the State*, HL 18, January 2009, para 177). An exception could also be made for the other emergency services who sometimes need to access subscriber data in order to identify persons involved in accidents, etc.

[57] Home Office Review of Counter-Terrorism Powers (Cm 8004, January 2011), p 29.

[58] Para 2.11.

[59] Ibid, para 4.12.

33. The possibility that 'directed' surveillance may prove highly intrusive was highlighted in *In re C*, in which the Divisional Court in Northern Ireland held that the use of surveillance to monitor privileged communications between lawyers and suspects in prison cells and custody suites was unlawful because of the lack of prior judicial authorisation.[60] However, although the subsequent 2010 order[61] introduced the requirement for such authorisation in order to monitor 'legal consultations' in places of detention, it is notable that it still adopted a location-based approach rather than one of substance. In other words, it is still permissible under RIPA to use directed surveillance of a privileged conversation that takes place in a town hall or an MPs office or a park bench, etc.

34. We therefore recommend that the definition of 'intrusive' surveillance be tightened, so that the former includes *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy. 'Directed' surveillance, in contrast, would be any use of covert surveillance that either does not or is not likely to involve a significant interference with a person's privacy.

35. For the same reasons outlined above in respect of interception and communications data, we also recommend that the power of the Secretary of State to authorise intrusive intelligence by the intelligence services under s41 RIPA should be repealed. Instead, *all* use of intrusive surveillance should be authorised by the Surveillance Commissioners or a judge of equivalent level.

36. As regards the use of covert sources, we note an increasing number of revelations in recent years concerning the conduct of undercover officers, including in particular members of the National Public Order Intelligence Unit, the National Domestic Extremism Unit, and the Metropolitan Police's Special Demonstration Squad. These have resulted not only in a series of investigations by HM Inspector of Constabulary, the National Crime Agency and the Independent Police Complaints Commission among others, but also several miscarriages of justice[62] and, in the most recent case, a settlement of £425,000 to a woman whose child was fathered by an undercover police officer.[63]

37. In our view, these cases further highlight the inadequacy of the internal self-authorisation model that underpins much of RIPA. We note, moreover, the 2011 recommendation of the then-President of the Association of Chief Police Officers, Sir Hugh Orde, that

---

[60] [2007] NIQB 101, subsequently upheld by the House of Lords in *In re McE* [2009] UKHL 15.
[61] The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI 2010/461).
[62] *David Robert Barkshire and others v The Queen* (Court of Appeal Criminal Division, unreported, 20 July 2011).
[63] See e.g. BBC News, "Met pays £425,000 to mother of undercover policeman's child", 24 October 2014.

judicial authorisation of undercover officers should be required in complex cases.[64] The Chief Surveillance Commissioner has also indicated that he was "also agreeable in principle to Commissioners giving prior approval to certain kinds of such activity by a [covert human intelligence source], provided that the OSC is given the appropriate resources to deal with the number of cases which arise and subject to any necessary legislation conferring the power".[65] We therefore recommend that the use of undercover officers should be authorised by a judge in any case where their conduct is likely to involve a significant interference with another person's privacy.

Encryption keys

38. The threat of terrorism has since the 1990s been cited by government officials as justifying the need for a statutory power to obtain encryption keys,[66] though the powers under Part 3 of RIPA were not brought into force until October 2007. Since then, it does not appear to have been widely used by either the police or the intelligence services and, when it has been used, it has mostly been used for non-terrorist offences such as child sex abuse.[67]

39. Although we consider that the power to obtain encryption keys is, in certain circumstances, a necessary one, there are a number of ways that the existing framework could be improved. First, Part 3 of RIPA is poorly-drafted. As we noted above, accessibility and certainty are both core requirements of the rule of law and the ECtHR has repeatedly made clear the need for "clear, detailed rules" and "accessibility and clarity" not only in the case of interception but also to "more general programmes of surveillance".[68] Secondly, permission to make a notice can only be made by a Circuit Judge, save where the encrypted material has been obtained under a warrant from or with the authorisation of the Secretary of State.[69] As with interception, communications data, and intrusive surveillance, we recommend that the Secretary of State should play no role in authorising surveillance. Instead, an encryption notice should only be authorised by a judge.[70] Thirdly, although there has already been some judicial consideration of the privilege against self-incrimination,[71] neither RIPA nor the Code of Practice make any allowance for journalistic material or material covered by legal professional privilege corresponding with the safeguards contained in PACE.

---

[64] Sir Hugh Orde, "Undercover Policing and Public Trust", 7 February 2011.

[65] 2011-2012 report, para 5.1.

[66] See e.g. Department of Trade and Industry, Paper of Regulatory Intent concerning Use of Encryption on Public Networks (June 1996).

[67] See e.g. the report of the Chief Surveillance Commissioner for 2009-2010 at para 4.11: "[The offence of] the possession of indecent images of children … is the main reason why section 49 notices are served. Other offences include: insider dealing, illegal broadcasting, theft, evasion of excise duty and aggravated burglary. It is of note that only one notice was served in relation to terrorism offences". See more generally JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011), paras 327-333.

[68] *Liberty and others v United Kingdom* (2009) 48 EHRR 1 at para 63.

[69] Paragraph 2 of Schedule 1 of RIPA.

[70] In cases involving the intelligence services and other sensitive cases, it may be more appropriate for the application to be made to a security-cleared High Court or Crown Court judge rather than a Circuit Courtjudge.

[71] See *R v S and A* [2008] EWCA Crim 2177 and *Greater Manchester Police v Andrews* [2011] EWHC 1966 (Admin).

Oversight

The Commissioners

40. In *Kennedy*, the ECtHR described the Interception of Communication's review of "a random selection of specific cases in which interception has been authorised" as "an important control of the activities of the intercepting agencies and of the Secretary of State himself".[72] The Bingham Centre agrees that the oversight provided by the Interception Commissioner - together with that provided by the Intelligence Services Commissioner and the Chief Surveillance Commissioner – constitutes an extremely important safeguard against the unnecessary or disproportionate use of surveillance powers. As valuable as this independent safeguard is, however, we consider that the oversight regime provided by the Commissioners suffers from a number of significant deficiencies.

41. First, it is clear that the remit of each Commissioner, taken together, does not provide comprehensive oversight of the exercise of surveillance powers under RIPA. The Interception of Communications, for instance, has no statutory remit in respect of interceptions under section 3 and has only agreed to provide oversight of interceptions in prisons on a "non-statutory" basis.[73] This does not, however, include other places of detention such as private prisons or secure mental health facilities, nor does it extend to the very broad power of communications service providers and operators of private communications networks to intercept communications for "the purposes connected with the provision or operation of a [telecommunications] service" under ss 3(1) and 3(3) respectively.

42. Secondly, the current framework defines the remit of each oversight Commissioner according to function in some cases and by agency in other cases. In practical terms, this means that surveillance of a privileged communication between a suspected terrorist and his lawyer may be subject to oversight by three different Commissioners, depending entirely on how it was authorised and according to which agency carried out the surveillance, i.e.:

    a. If the phone conversation was intercepted under Part 1 RIPA then the Secretary of State's warrant would be subject to review by the Interception of Communications Commissioner;

    b. If the phone conversation was monitored by way of a hidden microphone planted in the suspect's home by one of the intelligence services, then the Secretary of State's authorisation for intrusive surveillance under Part 2 RIPA would be subject to review by the Intelligence Services Commissioner; or

[72] *Kennedy*, para 166.

[73] See the 2002 report of Sir Swinton Thomas at para 59: 'I have been asked by the Home Office,

and have agreed in principle, to oversee the interception of communications in prisons'.

c. If the phone conversation was monitored by way of a hidden microphone planted in the suspect's home by the police, then review of the authorisation for intrusive surveillance under Part 2 RIPA would be subject to review by the Chief Surveillance Commissioner.

The potential for this piecemeal oversight also arises in other parts of RIPA: e.g. the use of encryption notices under Part 3 which has been reported on by all three commissioners. In our view, it is highly undesirable that the same intrusion could be subject to oversight by three different bodies, each with their own distinct procedure and approach, depending on the choice of methods and the agency involved.

43. Thirdly, it is apparent that both the Interception of Communications Commissioner and the Intelligence Services Commissioner are part-time posts, and inspect only a small sample of the warrants and authorisations made annually under Part 1 RIPA by the various Secretaries of State.[74] In his most recent report, for instance, the Interception of Communications Commissioner stated that he inspected approximately 600 applications for warrants made in 2013,[75] amounting to little more than 20% of the 2760 warrants issued that year. Although the Commissioner has defended this as a "sufficient representative sample of the individual warrants",[76] we note that each warrant embodies a decision by a member of the executive to invade the privacy of one or more persons (and in the case of a warrant under s8(4), potentially millions of people). It is therefore not acceptable, in our view, that approximately 4 in every 5 warrants, and more than 90% of authorisations to access communications data, are never looked at by a judge, even after the fact.

44. Fourthly, even when warrants and authorisations are scrutinized, it remains unclear what standard is applied by the reviewing Commissioner in each case, e.g. does he satisfy himself whether the interference with Article 8(2) was necessary and proportionate[77] or does he simply consider whether the Secretary of State's assessment of those factors was *Wednesbury* reasonable?

45. Fifthly, even in the unlikely event that the Interception of Communications Commissioner discovered that the Secretary of State had made a warrant that he considered to be unlawful, RIPA does not provide him with any power to quash the warrant. He may, of course, report the matter to the Prime Minister under s58(2) but the Prime Minister has the discretion to redact such information from the report laid before Parliament. Nor does

---

[74] House of Commons Home Affairs Committee, *Counter-terrorism* (HC 231, April 2014) at para 163: "The information given to us by the Commissioners indicate that they examine a small number of warrants under the current oversight system. The Intelligence Services Commissioner told us that in 2012 he had examined 8.5% of warrants. The Interception of Communications Commissioner told us that he had examined between 5% and 10% of the applications. He was not able to be more specific as he did not know how many applications there were."

[75] Para 3.36.

[76] Para 3.37.

[77] c.f. *Huang v Secretary of State for the Home Department* [2007] UKHL 11 at para 20.

the Interception of Communications Commissioner have the power to refer a possible breach of Article 8 ECHR tothe Investigatory Powers Tribunal.

46. For the above reasons, the Bingham Centre does not consider that the Commissioners overall provide "effective control" of surveillance powers under RIPA, save in the limited circumstances where those powers have already been subject to prior judicial authorisation (e.g. the use of intrusive surveillance where approved by the Surveillance Commissioners, or the use of directed surveillance by local authorities). In our view, extending judicial authorisation across the board would go a long way to reducing the administrative burden on the commissioners. While the burden will, of course, shift rather than disappear, the shift is worthwhile as it is of vital importance for control to be effective. Even so, it is apparent that the different oversight schemes are in need of rationalisation and we therefore recommend that the current functions be combined within a single, properly-staffed and funded body providing more coherent and effective oversight. We also recommend that this body have a broader remit to oversee the use of *all* surveillance powers by public bodies, rather than the current fragmented statutory regime. Although concerns have been expressed that putting oversight on a more permanent footing may result in less independent-minded candidates being available, we consider that it should be possible to devise a model that strikes an appropriate balance between independence and effectiveness. We note, for instance, that the Law Commission is chaired by a High Court or Appeal Court judge, serving for up to three years. We see no reason why appointment to chair the statutory oversight regime for surveillance powers should not be on a similar footing.

Investigatory Powers Tribunal

47. Just as the ECtHR in *Kennedy* praised the role of the oversight Commissioners, so too it commended the Investigatory Powers Tribunal as an "independent and impartial body, with its own rules of procedure" that constituted a "general safeguard" against the abuse of surveillance powers.[78] In addition, the ECtHR found that the procedures of the Tribunal did not "impair the very essence of the applicant's Article 6 rights", notwithstanding that the Tribunal considered his specific complaints in private without him being present, did not provide the applicant with any disclosure, did not afford him the opportunity to cross-examine any witnesses on the other side, and did not appoint a special advocate to represent his interests in any of the hearings from which he had been excluded.[79]

48. In our view, however, the decision of the ECtHR in *Kennedy* is not consistent with its own established jurisprudence on the justiciability of surveillance decisions under Article 6.[80]

[78] See *Kennedy*, paras 167 and 169.
[79] Ibid, para 184-190.
[80] See e.g. *Klass* at para 75: "the question whether the decisions authorising such surveillance under the [German statute] are covered by the judicial guarantee set forth in Article 6…must be examined by drawinga distinction between two stages: that before, and that after, notification of the termination of surveillance. As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6 … as a consequence, it of necessity escapes the requirements of that Article"; see also

More generally, while we accept that the Tribunal constitutes an essential safeguard against unlawful and disproportionate surveillance,[81] we are concerned that it is also severely flawed in a number of respects.

49. First, the proportion of applicants who are successful in their complaints before the Tribunal is extremely low – some 0.5% in the first decade of its operation.[82] In contrast, the annual success rate for complainants before other tribunals varies between 13% (mental health) and 41% (immigration and asylum).[83] In our view, the very poor success rate of complaints before the IPT does not necessarily reflect the quality of decision-making in the field of surveillance powers but rather almost certainly reflects the difficulty of bringing an effective challenge against the use of covert powers in a Tribunal in the absence of (i) proper notification requirements and (ii) any right to disclosure.

50. In *Klass*, the ECtHR conceded that the lack of any requirement on a public body to notify a person that they had been subject to surveillance following its conclusion meant that there was "in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality".[84] Despite this, the Strasbourg Court held that, although desirable, the absence of notification of surveillance did not breach the right to an effective remedy under Article 13 ECHR.[85] Although more recent cases have stressed the importance of notification requirements as safeguards against abuse of surveillance powers,[86] the ECtHR has yet to hold that notification is a *necessary* safeguard in such cases.[87] We note, however, that notification requirements are now a commonplace feature of surveillance laws in a great many jurisdictions including

---

the dissent of Lord Kerr in Tariq v Home Office [2011] UKSC 11 at para 128: "The entire point of surveillance is that the person who is subject to it should not be aware of that fact. It is therefore impossible to apply article 6 to any challenge to the decision to place someone under surveillance, at least until notice of termination of the surveillance has been given … It is precisely because the fact of surveillance must remain secret in order to be efficacious that article 6 cannot be engaged. It appears to me, therefore, that the decision in Kennedy ought to have been made on the basis that article 6 was not engaged because the issues that the case raised were simply not justiciable."

[81] See e.g. *Paton v Poole Borough Council* (IPT/09/01/C, 29 July 2010).

[82] See JUSTICE, *Freedom from Suspicion*, at paras 358-364.

[83] Ibid, para 359.

[84] *Klass* at p*ara* 57.

[85] Ibid, para 69.

[86] See esp. *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* [2007] ECHR 533 at para 57: "[U]nless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them."

[87] The issue is currently before the Court in the case of *Lüütsepp v Estonia* (46049/13).

Belgium,[88] Bulgaria,[89] Canada,[90] Germany,[91] Ireland,[92] the Netherlands,[93] New Zealand,[94] Sweden[95] and the United States.[96] In his 2013 report to the General Assembly on communications surveillance, moreover, the UN Special Rapporteur on Freedom of Expression stated:[97]

> *Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.*

51. We further note that the Codes of Practice on communications data and encryption keys under RIPA both make provision for notification where a Commissioner establishes that an individual has been "adversely affected" by any "wilful or reckless failure" by a public body. [98] In such cases, the Commissioner is required, "subject to safeguarding national security" to "inform the affected individual of the existence of the Tribunal and its role" as well as to "disclose sufficient information to the affected individual to enable him to effectively engage the Tribunal". It is unclear, however, why these notification requirements should be limited to only cases involving communications data and encryption keys, as well as why the threshold should be restricted to "wilful or reckless" failures. Rather than have the Commissioner make a determination of whether to notify in each case, we consider that the better approach would be to require mandatory notification in each case within a reasonable period (e.g. 6 months following the warrant or authorisation expiring), subject to a judge's decision that notification should be delayed on the basis that that individual's right to an effective remedy is outweighed by some specific investigative need that would otherwise be prejudiced by the disclosure. As with the

---

[88] See Belgian Constitutional Court, *case no. 145/2011*. 22 September 2011 at paras B.82-B92, in which the court held the lack of notification breached the right to privacy under Art 22 of the Belgian Constitution. [89] See *Lenev v Bulgaria* (41452/07, 4 December 2012) noting that section 34h of the Special Surveillance Means Act 1997 has been amended such that the supervising commission "must inform of its own motion persons who have been unlawfully subjected to secret surveillance, unless notification might jeopardise the purpose of the surveillance, allow the divulgation of operational methods or technical devices, or put the life or health of an undercover agent or his or her relatives or friends in jeopardy" (para 82).

[90] Section 196 of the Criminal Code provides for notification within 90 days of authorisation unless the judge is satisfied that investigations are ongoing or a subsequent investigation would be impeded. Notification cannot be delayed for more than 3 years.

[91] See e.g. *Klass* at para 19 and *Weber and Saravia v Germany* (54934/00, 29 June 2006) at para 136.

[92] Section 10(3) of the Criminal Justice (Surveillance) Act 2009.

[93] Article 34(1) of the Intelligence and Security Services Act 2002 requires notification after 5 years unless certain grounds are met.

[94] Sections 61 and 62 of the Search and Surveillance Act 2012.

[95] Section 11(a) of the 2008 law on Signals Intelligence (SFS 2008:717).

[96] 18 US Code § 2518(8)(d).

[97] UN Special Rapporteur on Free Expression A/HRC/23/40, 17 April 2013, at para 82. See also e.g. the International Principles on the Application of Human Rights to Communications Surveillance, May 2014.

[98] Communications Data Code of Practice at para 8.3. See also the similar provision in the Code of Practice for the Investigation of Protected Electronic Information at para 11.4.

Canadian Criminal Code, however, we recommend that there should be a maximum limit to the period of time for which notification can be delayed, e.g. 5 or 7 years.

52. As regards disclosure and the fairness of the IPT's procedures more generally, we accept that it is appropriate for the Tribunal to respect the agencies' policy of neither confirm nor deny (NCND) in the first instance, and particularly where the subject has not been notified of the surveillance in question. In our view, however, it is important to treat NCND as a starting point only, a defeasible principle that can be set aside where it becomes apparent to the IPT that it is necessary for the complainant to receive disclosure of material in order to effectively present his or her case. As the Vice President of the Court of Appeal held in a recent case, NCND is "not a legal principle" but rather a "departure from procedural norms" that "requires justification" in the same way as public interest immunity.[99] The framework of the IPT's procedures under Part 4 of RIPA, by contrast, do not – in our view – provide the Tribunal with sufficient flexibility to balance national security concerns with those of open justice and natural justice. Among other things, the IPT has no power even to make a declaration of incompatibility, has no formal power to appoint a special advocate to represent the interests of an excluded party, and indeed cannot even notify a party that a closed hearing has been held unless the other party consents. In this way, the framework under Part 4 compares unfavourably with the extensive case law that has developed in relation to closed proceedings in other courts and tribunals since 2001.[100]

53. We also consider that the ouster provision contained in s67(8) RIPA to be incompatible with the requirements of our common law constitution: if an appeal on a point of law is possible from other courts and tribunals employing closed procedures, we can see no good reason why the IPT should be immunised in this manner from the supervision of the higher courts. We therefore recommend that the IPT's procedural rules be significantly relaxed in order to enable much greater disclosure to complainants who have been subject to surveillance in order that they may bring an effective challenge, including sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded.

The Intelligence and Security Committee

54. Although the Intelligence and Security Committee provides important democratic oversight of surveillance powers and the activities of the intelligence services, we note that the accuracy of ISC reports has been the subject of judicial criticism in recent years, first in *R(Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs*[101] and subsequently in the report of Hallett LJ sitting as the Deputy Coroner in the inquest following the 7/7 bombings.[102]

[99] *Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 at para 20 per Maurice Kay VP. See also *DIL and others v Commissioner of Police of the Metropolis* [2014] EWHC 2184 (QB) para 42 per Bean J.

[100] See e.g. *AF v Secretary of State for the Home Department (No 3)* [2010] 2 AC 269; *Bank Mellat v HM Treasury (No 1)* [2013] UKSC 38.

[101] [2010] EWCA Civ 65 at para 168 per Lord Neuberger MR.

[102] Report of Deputy Coroner Hallett LJ under Rule 43 of the Coroner's Rules 1984 (6 May 2011), paras 110-116.

Following these criticisms, the constitution of the ISC was amended by Part 1 of the Justice and Security Act 2013. We note, however, that although the members of the ISC are now appointed by Parliament rather than the Prime Minister, a person cannot be eligible for appointment unless they have been nominated by the Prime Minister (s1(4)(a) of the 2013 Act). In addition, although the Committee reports now to Parliament instead of to the Prime Minister, it must nonetheless be sent first to the Prime Minister who may require the redaction of any material he considers to be prejudicial to the operation of the intelligence services (s3(4)). In our view, these restrictions are an unnecessary constraint on the Committee's oversight and should be removed.

Retention of communications

55. Notwithstanding that the judgment of the Grand Chamber in *Digital Rights Ireland* invalidating the Data Retention Directive was handed down in April 2014,[103] we note that the government's proposals to address this were not published until July and then enacted on an emergency basis in only three days. It is concerning that legislation on such an important issue was handled in such a manner. It remains unclear, moreover, whether the provisions of ss1-2 DRIPA are compatible with the CJEU's judgment. In our view, much will depend on the regulations and the particular retention notices made by the Secretary of State and we understand that this already the subject of legal challenge. At the very least, we recommend that the power to make retention notices should be removed from the Secretary of State. Instead, retention notices should be issued by a judge on application by the relevant public body seeking retention.

SUMMARY OF RECOMMENDATIONS

56. We recommend as follows:

(i) A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework.

(ii) Judicial authorisation should be required before any public body intercepts communications, accesses communications data, uses intrusive surveillance (including a covert human intelligence source), issues an encryption notice or a retention notice. The authorising judge should also have the power to direct the appointment of a special advocate to represent the interests of the subjects of surveillance in appropriate cases.

(iii) The existing power to intercept external communications under section 8(4) RIPA should be repealed. At the very least it should be severely curtailed. All warrants and authorisations must be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity.

[103] C-293/12, ECLI:EU:C:2014:238.

(iv) The statutory definition of 'intrusive' surveillance should be tightened to include *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy.

(v) The ban on the use of intercept material as evidence in criminal and civil proceedings should be lifted.

(vi) The number of public bodies able to access communications data should be curtailed.

(vii) The oversight functions currently discharged by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner should be combined into a single statutory oversight body. This body's remit should include oversight of the use of all surveillance powers by public bodies;

(viii) Any person who has been the subject of covert surveillance by a public body should be notified of that fact within a reasonable period following the conclusion of the surveillance, unless a judge is satisfied that that individual's right to an effective remedy is outweighed some specific investigative need that would otherwise be prejudiced by the disclosure;

(ix) The Investigatory Powers Tribunal should be granted the power to appoint special advocates to represent the interests of excluded parties, as well as make a declaration of incompatibility under section 4 of the Human Rights Act. Its procedural rules should also be relaxed to allow much greater disclosure to complainants who have been the subject of surveillance, so that they may bring an effective challenge. This should include sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded. The unsuccessful party should also have a right of appeal to the Court of Appeal on a pointof law;

(x) The statutory requirement that candidates for the Intelligence and Security Committee must first be nominated by the Prime Minister in order to be eligible for election should be repealed, as should the power of the Prime Minister to prevent the Committee from publishing material that it considers to be in the public interest to disclose.

November 2014

APPENDIX: BINGHAM CENTRE EXPERT SEMINAR, 1 OCTOBER 2014

On 1 October 2014, the Bingham Centre for the Rule of Law held an evening conference on the subject of the Investigatory Powers Review led by the Independent Reviewer of Terrorism Legislation, David Anderson QC. Chaired by Eric Metcalfe of Monckton Chambers and the Bingham Centre, the event consisted of three panels: (I) Interception Warrants; (II) Communications Data; and (III) Oversight.

The evening began with an introduction to the Review by David Anderson, and was followed by a discussion of Section 8(1) warrants by Helen Mountfield QC, and Section 8(4) warrants by Matthew Ryder QC, both of Matrix Chambers. Panel II consisted of a discussion of Access to Communications Data under Part 1, Chapter 2 of RIPA by Graham Smith of Bird & Bird, followed by Gillian Phillips, Director of Editorial Legal Services at The Guardian on the subject of RIPA and Professional Privacy. Finally, Panel III concluded with presentations from Tom Hickman of Blackstone Chambers and the Bingham Centre and Eric Metcalfe on the Investigatory Powers Tribunal and the oversight Commissioners and the Intelligence and Security Committee.

The event included lively and and expert debate from the floor and was followed by a reception. The Bingham Centre is grateful to Macfarlanes for hosting the event.

List of Attendees

Name	Organisation
Mr Chris Acton	Macfarlanes
Mr David Anderson QC	Independent Reviewer of Terrorism Legislation
Mr Benjamin Baltzer	Embassy of the Federal Republic of Germany
Mr Martin Bentham	Evening Standard
Dr Jessie Blackbourn	Kingston University
Mr Owen Bowcott	The Guardian
Ms Jennifer Bruce	Ofcom
Mr Tom Bullmore	Treasury Solicitor's Department
Mr Jude Bunting	Doughty Street Chambers
Ms Elinor Buxton	Foreign & Commonwealth Office
Lord Carlile CBE QC	Gray's Inn
Ms Hannah Carter	Ofcom
Mr Rupert Casey	Macfarlanes
Ms Jo Cavan	Interception of Communications Commissioner's Office
Mr Martin Chamberlain QC	Brick Court Chambers
Mr Jan Clements	The Guardian
Mr Martin Coombes	Macfarlanes

Mr Gordon Corera	BBC
Mr Jeremy Courtenay-Stamp	Macfarlanes
Ms Gail Crawford	Lathan & Watkins LLP
Ms Aalia Datoo	Macfarlanes
Dr Andrew Defty	University of Lincoln
Ms Adriana Edmeades	Privacy International
Mr Charlie Edwards	RUSI
Mr Charles Farr OBE	Home Office
Mr Daniel Futter	Metropolitan Police, Directorate of Legal Services
Ms Tessa Gregory	Leigh Day
Mr Stephen Grosz QC (Hon)	Bindmans; Bingham Centre Fellow
Ms Gabrielle Guillemin	ARTICLE 19
Ms Laila Hamzi	Bingham Centre for the Rule of Law
Ms Swee Leng Harris	Bingham Centre for the Rule of Law
Dr Tom Hickman	Blackstone Chambers; Bingham Centre Fellow
Mr Jess Hinings	Ofcom
Ms Sandra Homewood	Bingham Centre for the Rule of Law
Mr Ben Hooper	11 King's Bench Walk
Mr Henry Hughes	187 Fleet Street
Mr Mark Hunting	Ropes & Gray LLP
Mr Ben Jaffey	Blackstone Chambers
Mr Tim Johnston	Brick Court Chambers
Ms Sarah Kavanagh	NUJ
Mr Bernard Keenan	LSE
Mr Eric King	Privacy International
Ms Izza Leghtas	Human Rights Watch
Mr Paul Lomas	Freshfields
Ms Gemma Ludgate	Special Advocates Support Office
Professor Andrew Lynch	University of New South Wales
Mr Daniel Machover	Hickman & Rose
Mr Iain Mackie	Macfarlanes
Ms Jennifer Macleod	Brick Court Chambers
Mr Andy Mather	Macfarlanes
Dr Eric Metcalfe	Monckton Chambers; Bingham Centre Fellow

Ms Helen Mountfield QC	Matrix Chambers
Sir Jon Murphy QPM	Chief Constable, Merseyside Police
Sir David Omand GCB	King's College London
Ms Angela Patrick	JUSTICE
Ms Gillian Phillips	The Guardian
Mr Mark Powell	HM Inspectorate of Constabulary
Ms Charlotte Powell	Furnival Chambers
Dr Tristram Riley-Smith	Centre for Science & Policy, Cambridge University
Mr Matthew Ryder QC	Matrix Chambers
Mr Naz Saleh	Metropolitan Police
Ms Helen Shaw	Inquest
Ms Jessica Simor QC	Matrix Chambers
Mr Graham Smith	Bird & Bird
Ms Justine Stefanelli	Bingham Centre for the Rule of Law
Mr Dominic van der Wal	Special Advocates Support Office
Mr James Welch	Liberty
Ms Harriet Wistrich	Birnberg Peirce & Partners
Mr Julian Wright	Metropolitan Police

Birnberg Peirce and Partners

We write in respect of the recently announced review into the operation of Investigatory Powers which we understand is limited only to parts 1 and 4 of RIPA.

We represent eight women who, over a period of 25 years, were all in long term intimate relationships with men they have subsequently discovered were undercover police officers. They have all been significantly harmed by the gross abuse of power and the level of deceit they were subjected to. Three of these eight women had relationships with an undercover police officer after the enactment of RIPA and those three women have conducted satellite litigation which has raised the issue as to whether it is within the statutory construction of RIPA that officers could have an intimate sexual relationship with a member or associate of a target group whilst in his undercover guise and whether the Investigatory Powers Tribunal (IPT) has jurisdiction to determine the claims brought under s. 7(1), Human Rights Act 1998.

The ruling by Mr Justice Tugendhat in the High Court ([2013] EWHC 32 (QB) acknowledged that the claims concern "the gravest interference with their fundamental rights recognised by the common law", and also that "some sexual relationships established or maintained covertly might amount to degrading treatment" which amounted to an interference with a fundamental right and as such was incapable of being authorised under Part 2 of RIPA. However it was held that other sexual relationships might only amount to no more than an interference with the right to privacy which is capable of being authorised under Part 2 of RIPA.

The Judge then ruled that "what is or is not a sexual relationship, or an intimate sexual relationship, is too broad and uncertain a concept for the whole range of such possible relationships to be characterised as degrading, and so outside the scope of any possible authorisation", and that "I find nothing in the provisions of s.30, or the Statutory Instrument made under it, to support the submission that Parliament did not contemplate authorisations of such relationships." The Court of Appeal upheld his judgment in AJA and others -v- The Commissioner of Police for the Metropolis [2013] EWCA Civ 1342

As such this leaves the alarming conclusion that RIPA legislation permits sexual relationships, without setting any clear boundaries about what is considered acceptable and what amounts to degrading treatment.

The Claimants are now seeking permission from the Supreme Court to appeal the Court of Appeal decision on this matter. However, if this judgment is upheld and in any event, the result of this interpretation of the statutory construction of RIPA is deeply worrying in the light of the evidence that serious harm can be caused to members of the public as a result of this form of surveillance activity.

I am enclosing some submissions drafted by my clients submitted to Rt Hon Damian Green MP, the then Minister for Policing and Criminal Justice, who had invited contributions to a recent consultation of the Codes of Practice of RIPA aimed at amending that guidance to ensure that such conduct should not occur in the future. These submissions set out the extent to which and range of violations arising from the collective experience of these women and indicate an imperative that legal reform is required. Unfortunately, our contribution to the consultation appears to have been ignored or judged irrelevant, since the proposed amendments still to be debated by Parliament do not deal with the issues my clients have raised.

Whilst it is understood that Parts 1 and 4 of RIPA do not directly cover the activities of undercover police officers and the more broadly defined category of covert human intelligence sources, part 4 does provide for safeguards with a view to preventing misuse or abuse of

investigatory powers. Further to our email exchange last week, I would wish to draw to your attention in particular to one very surprising aspect of the statutory construction of RIPA which does directly impinge on your review.

In our submissions to the High Court or Court of Appeal, we produced a table indicating the hierarchy and level of authorisation required for different forms of intrusive surveillance by the state. Certain types of activity require authorisation from the very highest level, for example interception of communication requires authorisation from the Secretary of State. On the other hand, the authorisation of direct surveillance, including the activities of a Covert Human Intelligence Source, require only the authorisation of somebody at the level of a Chief Superintendent. It was our argument that given the clearly highly intrusive nature of an intimate sexual relationship by someone presenting as a political activist but really an undercover police officer, parliament cannot have intended that such officers would be authorised to engage in such conduct. If it had so intended that this was a possibility, then we consider that there is an inherent inconsistency in the statutory framework of RIPA.

In respect of your review, we suggest that for any long term deployment of an undercover officer, the level of authorisation should be increased to the Secretary of State since that deployment is clearly capable of being far more intrusive than the interception of communications. We hope that in presenting your overview of the relevant Parts of this legislation, that you could draw attention to this apparent inherent flaw in the statutory regime and the urgent need for reform in respect of Part II of RIPA.

Harriet Wistrich
October 2014

Submission on new Covert Human Intelligence Sources Code of Practice and Covert Surveillance Code of Practice

Introduction

We are a group of 8 women bringing a legal action against the Commissioner of the Metropolitan Police arising from the intrusion into our lives by undercover officers and we are responding to the consultation on proposals to update the Covert Human Intelligence Sources Code of Practice and the Covert Surveillance Code of Practice.

The following points for the consultation are made without prejudice to our view that there are profound structural flaws within RIPA, which suggest that the whole Act requires a radical overhaul. Nor does our participation in this consultation constitute tacit acceptance of the use of undercover policing against political dissent. We simply wish to try and ensure that the abuses we experienced cannot happen again.

We note that despite the controversy over the issue of undercover relationships in the past couple of years, the Codes of Practice fail to make any mention of intimate and sexual relationships.

On your website it states that "both codes of practice have greatly improved control and oversight of the way public authorities use covert investigatory techniques, in order to protect our right to privacy." Having had our privacy intruded upon to a huge and damaging degree we feel that these guidelines fail to address the issues raised by our claims and fail to offer any increased protection to the public.

The changes proposed to the Codes of Practice are not sufficient to prevent the kinds of abuses that have been perpetrated by undercover officers like Mark Kennedy and Marco Jacobs, who were operating under very similar Codes of Practice. It is irrational and represents a dereliction of duty for new guidelines to ignore this behaviour, which has been called "unacceptable and grossly unprofessional" by Jon Murphy, head of ACPO (January 2011).

In the light of inconsistent statements by senior police and ministers** on the subject of sexual relationships, a duty is owed by the government to the public (and to officers) to ensure the regulations are clear. The situation as it stands currently gives free reign to officers and their handlers, and in view of the fact that women have been disproportionately affected by these relationships, a failure to introduce measures to prevent further abuse, amounts to institutional sexism.

** Inconsistent statements on the policy in respect of sexual conduct by undercover officers can be found detailed here:
http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/837/837we02.htm

Proposed addition to Codes of Practice

In our view, in order to provide protection to the public against this abuse, the Codes of Practice need to incorporate a clear statement so officers know from the start of their deployment that sexual and intimate relationships while undercover are not acceptable. We propose that the following statement be added to the text of para 2.13 (p7):

"Officers are expressly forbidden from entering into intimate or sexual relationships whilst in their undercover persona."

Such a statement is necessary for the following reasons:

1) Intimate and sexual relationships by undercover officers concealing their real identity from the other person/s in the relationship/s represent a clear violation of the right to respect for private and family life (Art 8) and the right not to be subject to inhumane and degrading treatment (Art 3). When used by officers infiltrating campaigning and political organisations, they also represent a violation of the right to freedom of expression (Art 10) and freedom of assembly and association (Art 11).

2) Intimate and sexual relationships by undercover officers concealing their real identity from the other person/s in the relationship/s causes serious long-term harm and psychological trauma to those persons and others close to them.

3) Such relationships additionally harm the officers' families and the officers themselves.

4) Intimate and sexual relationships by officers concealing their true identity from other person in the relationship amounts to a gross invasion of an individual's fundamental common law right to personal security.

5) The tactic as it has been used, plainly has had and will have a discriminatory effect on women and is thus prohibited by Article 14 ECHR.

6) Under Section 74 of the Sexual Offences Act 2003, a person can only consent to sex if she "agrees by choice, and has the freedom and capacity to make that choice". Recent case law adds strength to the argument that undercover officers would be committing sexual offences if they enter into a sexual relationship. (*Assange v Swedish Prosecution Authority* [2011] EWHC 308 and *R v McNally* [2013] 2 Cr.App. R.28). It has also been suggested by Chief Constable Mick Creedon in Operation Trinity Report 2 that offences of Misconduct in Public Office may apply. This means that sexual relationships *cannot* be permitted under these codes, whatever the level of authorisation. This needs to be made clear.

7) Sexual relationships may produce children and have done in at least two of the reported cases. This means that the tactic poses a risk to women's bodies and could also have a profound effect on the rights of a child as contained in the UN Convention on the Rights of the Child (UNCRC). Article 7 of the UNCRC requires children to be given the right to know their parents. It is difficult to see how the use of a tactic which carries with it the risk that a child will be born to an undercover police officer who will disappear into thin air at a certain stage in the child's life could be compatible with the UNCRC.

8) Conversely, where relationships are long-lasting, and the officer is unwilling to have children, they have an effect on a woman's right to have children, as protected by the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), since women's fertility is so much more short-lived than that of men.

9) There is clearly a disproportionate use of the tactic against women. The failure to provide any guidance in relation to sexual relationships itself has a discriminatory impact on women because it makes it more likely that their rights will be unjustifiably interfered with. The impact on women also gives rise to the need to conduct an equality impact assessment in relation to the publication of any new Code of Guidance. No such Equality Impact Assessment has to our knowledge been produced.

Further background

1) **Article 3 rights are absolute or unqualified human rights** – it is not possible to authorise someone to violate an unqualified human right under any circumstances. We note that in a recent High Court judgement, Justice Tugenhadt stated that a physical sexual relationship, which is covertly maintained, is more likely to fall into the category of degrading treatment, “depending on the degree and nature of the concealment or deception involved”.

2) **Article 8, 10 & 11 rights are qualified rights, but interference with qualified rights is permissible only if:**

a) **there is a clear legal basis for the interference with the qualified right that people can find out about and understand**.

We note that there is nothing in law which states that if a police officer suspects an individual of involvement in a crime or with a political movement, that officer is entitled to have a sexual relationship with the person to try to find out.

b) **the action/interference is necessary in a democratic society.**

Sexual and intimate relationships cannot be said to be necessary – It was asserted by Nick Herbert in June 2012 that "to ban such actions would provide a ready-made test for the targeted criminal group to find out whether an undercover officer was deployed among them." We believe this to be a ludicrous argument designed to allow abuse to continue. There are a multitude of reasons why any individual might decline to become intimate with another person. Such reasons are given in every day life and would not lead to an assumption that the person declining was an undercover officer.

In any event, such an argument would not be tolerated in respect of murder or child abuse, so why should it be tolerated in respect of abuse of women?

Further a defence of necessity and self-defence already exists in British law therefore any officer genuinely in fear of his or her life and forced by circumstances into breaking the prohibition would be able to argue this in their defence.

c) **the action/interference is proportionate to what is sought to be achieved by carrying it out.** The action or interference must be in response to 'a pressing social need', and must be no greater than that necessary to address the social need. Given the level of invasion of privacy and the serious psychological harm caused by such relationships they would clearly fail the hurdle of proportionality.

3) **The rights of women to autonomy in reproduction are protected by the Convention on the Elimination of All Forms of Discrimination Against Women** (CEDAW), Article 16(1) of which provides: States Parties shall take all appropriate measures to eliminate discrimination against women in all matters relating to marriage and family relations and in particular shall ensure, on a basis of equality of men and women:

(a) The same right to enter into marriage;
(b) The same right freely to choose a spouse and to enter into marriage only with their free and full consent;
(c) The same rights and responsibilities during marriage and at its dissolution;
(d) The same rights and responsibilities as parents, irrespective of their marital status, in matters relating to their children; in all cases the interests of the children shall be paramount;
(e) The same rights to decide freely and responsibly on the number and spacing of their children and to have access to the information, education and means to enable them to exercise these rights.

4) **Article 3 of the UNCRC** provides that "*In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."* **Article 7** states: "*The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and. as far as possible, the right to know and be cared for by his or her parents.*

5) German Police internal guidelines expressly forbid the use of intimate or sexual relationships for the purpose of gathering information because this would violate basic privacy rights ("Kernbereich privater Lebensgestaltung"). This applies to undercover investigators as well as informants employed by the federal authorities. If it is possible to ban this tactic in another European country without risking a "ready-made test" for a targeted group then there is no reason not to implement such a ban here.

Section on Collateral Intrusion (p12)

In our experience the depth of the intrusion into our lives also meant a deep intrusion into the lives of family members and close friends. For example, undercover police officers "infiltrated" deeply emotional family gatherings such as funerals, weddings and birthday celebrations. The psychological harm inflicted, not only on us, but on close members of our family (including infirm, elderly relatives) cannot be justified.

Such intrusion is referred to in the guidelines as "Collateral Intrusion" and, perversely, its authorisation appears to require less rigorous tests than intrusion into the lives of "suspects". Collateral Intrusion is, it seems, a euphemism for violating the fundamental human rights of people who are not even the specific subjects of surveillance, without any real consideration of the psychological damage that such deep deceptions might cause.

As can be seen from some of the authorisations for the activities of Mark Kennedy, it was considered that any "like minded activist" was a valid target for infiltration, and so further authorisation was not sought for their inclusion into the operation, regardless of their relevance to any investigation (and despite such an approach being a clear interference with Article 10 & 11 rights). It is also evident from documents that have come to light thus far that the extended family of political activists were also considered 'fair-game'. The Codes of Practice have not altered in any meaningful way to ensure that this behaviour does not continue.

In the same way that we don't consider that forming intimate sexual relationships could ever be considered necessary or proportionate, it is always wholly inappropriate for a police officer to insert themselves into extended families, in the way that being part of long-term relationships would necessitate.

In our view every individual whose Article 8 Human Rights may be breached by an operation should be afforded the respect of having the merits of that intrusion specifically considered and recorded, including the specific reasons why it is considered necessary and proportionate.

Levels of authorisation

In terms of intrusiveness, entering into deceitful long-term relationships and/or moving into people's homes and becoming party to the most intimate details of their private lives is quite clearly more intrusive than the interception of post and telephone calls, and the positioning of recording devices in people's homes or cars. The authorisation requirements should therefore be at least as stringent. It is inconceivable that despite increases in levels of authorisation provided for in these codes of practice, it is still the case that a phone tap needs greater authorisation than a CHIS.

It is still the case that whilst 'Warrants signed in person by the Secretary of State, authorisations from the Secretary of State or prior approval from a Surveillance Commissioner or judge' are required for what are considered the most intrusive methods of surveillance, it is not a requirement for the deployment of Covert Human Intelligence Sources. Whilst it is never acceptable to form intimate long-term relationships whilst operating undercover, it is still plainly absurd to consider a CHIS less intrusive than a phone tap in many cases.

To assist with understanding the impact of this type of intrusion on people's lives, we attach our evidence presented to the Home Affairs Select Committee, as well as our Letter before Claim Given this evidence it is clear that the most intrusive methods of surveillance used to date are not adequately dealt with by RIPA. These Codes of Practice should be changed to ensure that the abuses we have suffered would not be allowed in future.

ACCOUNTABILITY

This public consultation is taking place in the shadow of a consistently obstructive approach by the police to any public criticism. Their attitude to our cases has been to refuse to provide a properly pleaded defence or standard disclosure, even refusing to confirm or deny that the officers involved were in fact working for the police. Combine this with the recent allegations of corruption and cover-ups surrounding inquiries into cases such as Stephen Lawrence and Hillsborough, amongst others, and revelations about the shredding of documents pertaining to controversial police activity, the public perception of police accountability is low.

It is clear that the Codes of Practice as they applied to the NPOIU and the Kennedy operation, and as they now stand, will not be enough to ensure accountability. They must not be used to provide immunity from public scrutiny when wrong decisions are made, as has so patently happened in the past.

We must never lose sight of the fact that intrusive surveillance violates fundamental human rights. The test of whether something is 'proportionate or necessary' alone hasn't

been sufficient to prevent abuse of position by undercover officers in the past.

The most rigorous standards possible must be applied to ensuring the enforceability of these guidelines and other laws relating to the use of CHIS. Those who make the decision to violate someone's Human Rights under these Codes of Practice must be fully accountable to the public.

Caspar Bowden

Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament

Caspar Bowden is an independent advocate for information privacy rights, and public understanding of privacy research in computer science. He is a specialist in EU Data Protection, European and US surveillance law, PET research, identity management, and information ethics. He is author of 2013 EU Parliament inquiry briefing[1] on the US FISA law, and co-authored the 2012 Note on privacy and Cloud computing[2] (which anticipated the infringements to EU data sovereignty disclosed by Edward Snowden). For nine years he was Chief Privacy Adviser for Microsoft for forty countries, and previously co-founded and was first director of the Foundation for Information Policy Research (www.fipr.org). He was an expert adviser for UK Parliamentary legislation, author of the RIP Act Information Centre (**www.fipr.org/rip/**), and co-organized six public conferences on encryption, data retention, and interception policy. He has previous careers in financial engineering and risk management, and software engineering (systems, 3D games, applied cryptography), including work with Goldman Sachs, Microsoft Consulting Services, Acorn, Research Machines, and IBM. He founded the Award for Outstanding Research in Privacy Enhancing Technologies, is a fellow of the British Computer Society, and a member of the advisory bodies of several civil society associations.

There is no Executive Summary

The ISC would welcome written evidence on the following issues:

a) What balance should be struck between the individual right to privacy and the collective right to security?

1. Balance is a misleading metaphor. It tends to connote an unstable equilibrium with a single balance point on a linear scale. The policy options may include combinations resulting in different equilibria which are metastable, stable or unstable in the context of post-Snowden policy on surveillance.
2. For example, one reaction to Snowden might be to intensify surveillance and provide GCHQ with authority[3] to monitor every webcam in every laptop in the UK. If done overtly, this would likely produce a cowed population living under a sense of oppression, but amenable to further intensification of surveillance down a slippery slope. If done covertly, it raises the question why is that intuitively unacceptable (assuming it is), yet qualitatively similar surveillance of private life through metadata analysis (see below) seems more politically palatable? Does this merely reflect public and legislative (lack of) comprehension or technical imagination?

[1] *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, 16-09-2013, Caspar Bowden, intr. Didier Bigo http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

[2] *Fighting Cyber Crime and Protecting Privacy in the Cloud*, 15-10-2012, Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, Amandine Scherrer http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf

[3] This might even be possible today depending on nice interpretations of the interactions of the Intelligence Services Act and RIPA

3. Another option would be to end blanket collection of metadata, and switch to a regime of targeted preservation of metadata about defined suspect groups on a lawful basis. This might assuage public concerns, and leave a bright and comprehensible line for public understanding of the permitted limits of mass-collection.
4. Therefore a key factor in deciding "balance" is the long-term effect on political and democratic culture, and maximising short-term public consent to the demands of a security apparatus is not necessarily the wisest course, given that we are in uncharted waters.

How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras?

5. The Internet is not a public space, it is composed of many layers of private, social and public realms. CCTV surveillance is both overt and confined to public space, or private and social spaces lawfully subject to another's control. In contrast, the controversial aspects of state mass-surveillance are that it is covert and conducted over wholly or partially private spaces of data and communications.
6. I draw ISC's attention to my 2002 paper on ATCSA data retention[4], which is based on the metaphor that retention is like having a CCTV camera installed "inside your head" i.e. that it invades the subjective interior space of our thoughts and intentions, because these can be inferred from Internet and other metadata.

To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security?

7. It is incompatible with human rights in a democracy to collect all communications or metadata all the time indiscriminately. The essence of the freedom conferred by the right to private life is that infringements must be justified and exceptional. As the Romanian constitutional court[5] expressed it, the continuous limitation of the right to privacy [implied by mass-collection of metadata] empties the principle, by making the exception into the rule.
8. This principle against blanket data collection might be suspended in time of war or concrete imminent threat (as found by the German Constitutional Court in their *Rasterfahndung* decision[6]) but it cannot be the normal mode of surveillance in a democracy.
9. It is a strange fact that the obvious alternative policy to blanket **retention** has never been explored or publicly developed by the Home Office in 15 years, that of targeted and selective **preservation** of metadata about a defined (but dynamic) list of suspects. In fact this legal capability is provided in Pt.1 Ch.2 of RIPA, and is necessary to give effect to obligations under the Council of Europe Cybercrime Treaty. However these powers are generally only used in particular investigations, because of course UK policy developed to ensure such data was retained about the entire population.
10. However to assess whether blanket data retention is proportionate in the sense of

[4]Caspar Bowden, *CCTV for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation*, 1 Duke Law & Technology Review 1-7 (2002) http://scholarship.law.duke.edu/dltr/vol1/iss1/47
[5]E Kosta, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, (2013) 10:3 SCRIPTed 339 http://script-ed.org/?p=1163
[6]BVerfG, 1 BvR 518/02 vom 4.4.2006, Absatz-Nr. (1 – 184), http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html

the Human Rights Act requires a comparison to a hypothetical alternate regime in which preservation powers are exercised systematically over a target list that can be rationally justified by criminological research. For example, for offences for which recidivism is commonplace, it could be proportionate to release offenders on license under the condition of metadata preservation (with deterrent penalties for evasion).

11. If it is argued that such targeted preservation could stigmatize certain groups or that data about innocent persons would be caught, it must be pointed out that is much better than the current situation in which everybody's data is collected indiscriminately all of the time for no particular reason whatsoever.

12. Suppose that 95% of the effectiveness of the data retention regime could be achieved by intelligently targeting 1% of the population? It would be very hard to argue that increasing the amount of data one hundred times to achieve an extra 5% effect, was justifiably proportionate

13. The residuum of 5% would include "hard cases" of opportunistic crime and terrorism that might have been prevented, but in a more limited sense than usually understood. Access to the "time machine" provided by blanket retention can only help investigate terror networks and the causes of terrorist crimes. They cannot prevent acts of terrorism infallibly merely because data about everyone is being collected.

14. This then is the true balance: the breaching of the principle against blanket collection which voids the essence of the right to private life, or a lawful regime of targeted and proportionate preservation, which nevertheless might result in a residuum of crimes that might have been prevented or detected under a blanket retention regime.

15. Law enforcement agencies' appraisal of necessity cannot be taken at face value. In evidence to the Joint Committee on the Communications Data Bill, the Interception Commissioner pre-emptively distanced himself from "case studies" included in his annual report which he said were provided by the Home Office. In my evidence submission[7] I demonstrated how five out of six studies obviously failed to demonstrate necessity (the other was inconclusive), and that another anecdote offered by police in oral evidence was diametrically misleading.

How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?

16. The distinction is not a simple one and cannot be made by assigning a sensitivity level to data types in isolation.

17. The pattern of association between individuals and websites and geographic locations reveal a map[8] of private life which includes intimate and personal contacts, political activities, and business and professional relationships[9].

---

[7] Caspar Bowden , 23rd August 2012, *Submission to the Joint Committee on the draft Communications Data Bill* http://www.parliament.uk/documents/joint-committees/communications-data/written%20evidence%20Volume.pdf

[8] CCTV inside head ibid.

[9] Evidence of Prof. Ed Felten to Senate Judiciary Committee hearing on *Continued Oversight of the Foreign Intelligence Surveillance Act*, October 2, 2013 www.cs.princeton.edu/~felten/testimony-2013-

18. Global-scale databases of such relationships have been assembled on non-US citizens[10] by the NSA since at least 9/11, and the power to analyse and exploit such information automatically for foreign policy and political[11] purposes has been demonstrated in Snowden material

19. In contrast, speech-recognition of continuous voice streams (without training for particular speakers and at telephone quality bandwidths) remains a very hard problem in computer science[12]. However in the popular culture and early para-politics of the surveillance state, the main threat was portrayed as coming from computers which could scan and transcribe human speech. This image of the surveillance threat turned out to be a dead-end, but still colours public discourse.

20. It is harder to conceive of the surveillance power of traffic (metadata) analysis because of its scale and abstraction. Data-mining systems for national security use are designed to link any common identifying numbers of any kind, and look for correlations, geographical intersections of location data[13], and patterns in online social relationships. Unless special precautions are taken, few personal secrets of everyday life would withstand close analysis of metadata.

21. Critics of state mass-surveillance made these arguments[14] before the emergence of online social networks and smart-phones (and post-9/11 stimulus to the surveillance-industrial complex) but in 2000 legislators seemed content that RIPA did not mandate blanket data retention, and Labour Minsters made three promises they would not do so[15].

22. The Labour administration broke these pre-election promises after 9/11, and debate on the mandatory data-retention provisions in Ch.11 ATCSA (the "UK PATRIOT Act") resulted in the longest game of Parliamentary ping-pong between Lords and Commons in 2001, ending in the passage of a mangled version of an amendment devised by the author. The intention was to restrict data retention to that which was necessary for national security, leaving open the interpretation of how broadly or selectively this might be done, but with the tacit implication that blanket retention was unlawful.

23. In 2002 the Information Commissioner obtained an Opinion from Ben Emmerson QC which essentially approved that the (mangled wording of the) national security purpose in ATCSA could necessitate blanket collection, and decided not to get involved. This was a momentous point in UK data retention policy, but the

---

10-02.pdf

[10] *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, by James Risen and Laura Poitras, New York Times September 28, 2013 http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=2&_r=0&smid=tw-bna&pagewanted=all

[11] *Snowden Docs: British Spies Used Sex and 'Dirty Tricks'*, NBC News Feb 7th 2014, by Matthew Cole, Richard Esposito, Mark Schone and Glenn Greenwald http://www.nbcnews.com/news/investigations/snowden-docs-british-spies-used-sex-dirty-tricks-n23091

[12] As opposed to speaker identification via a voiceprint, which has been feasible and deployed since 1980s.

[13] *NSA tracking cellphone locations worldwide, Snowden documents show* (CO-TRAVELER) Washington Post 4th Dec 2013, by Barton Gellman and Ashkan Soltani 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

[14] *Unprecedented Safeguards For Unprecedented Capabilities* - Caspar Bowden, remarks for Hoover Institution National Security Forum Conference, 7th Dec 1999 http://www.fipr.org/publications/hoover.html

[15] CCTV inside head 2001 ibid.

reasoning has only been publicly available[16] following a recent FOI request to the ICO.

b) 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.

24. The most glaring lacuna in the legal regime is any regulation of the modality of analysis of data in bulk. Data processing for national security purposes is exempted from almost all control under the Data Protection Act 1998[17]. The Interception Commissioner could in theory object that certain forms of data-mining were incompatible with the Human Rights Act, but there is no evidence he has done so, and this would require him to construct novel and complex theories of technology- dependent jurisprudence in isolation and in secret. Any complaint to the Investigatory Powers Tribunal is unlikely to reach these arcana, as the complainant (and the IPT) would have to know something about the complex systems involved to raise the issue.

25. In general, once data has been lawfully acquired for national security processing there are no (publicly known) limitations on the nature of algorithms or their scale of application which are considered lawful or unlawful, other than the familiar ECHR rubrics of necessity and proportionality.

c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

26. One of the least understood or examined parts of RIPA is s.16, which purportedly deals with "extra safeguards" in respect of mass-surveillance of "external" communications. The author wrote two[18] briefing papers as House of Lords Adviser to Opposition parties which resulted in substantial debate of this clause.

27. s.16 is drafted with fiendish complexity[19], but essentially creates a "third kind" of warrant apart from the ordinary "domestic" interception warrant for use inside the UK, and the GCHQ "trawling warrant" for external communications. The third kind of warrant authorizes GCHQ to scan all the nominally external communications it captures, to target a **person** known to be inside the UK. It was thus not a safeguard at all, but a hugely significant increase in powers beyond the popular conception that GCHQ was only involved in foreign and international surveillance. It is fair to say that almost no members of either House or the public or media appreciated this at the time of legislation (or subsequently). Despite attempts to explain to news media, it was apparently just too complicated to report.

28. As was already foreseen in the debates[20] in 2000, in practice external

---

16 https://www.whatdotheyknow.com/request/gcs_opinion_on_data_retention_in

17 s.28 http://www.legislation.gov.uk/ukpga/1998/29/section/28

18 http://www.fipr.org/rip/CertificatedAndOverlapping.htm and http://www.fipr.org/rip/OverRideCertificates.htm

19 A senior government official confirmed to me privately that it was intentionally drafted for maximum obscurity

20 *Lords Hansard 19 Jun 2000 : from Column 97* http://www.publications.parliament.uk/pa/ld199900/ldhansrd/vo000619/text/00619-20.htm and *Lords Hansard 12 Jul 2000 : from Column 318* http://www.publications.parliament.uk/pa/ld199900/ldhansrd/vo000712/text/00712-21.htm

communications might contain a huge amount of data about persons and activities wholly within the UK, a situation much exacerbated since by the concentration of online services in a few big US-based companies.

29. The Interception Commissioner has never remarked or reported on the use of s.16, nor has there been any other policy or legal commentary of significance since enactment. Yet it seems likely that the interpretation and use of s.16 is critical to understanding the impact of the reported TEMPORA system on the privacy of those within the UK

30. s.16 appears to have been designed to close a leap of logic by Lord Lloyd in the first[21] Interception Commissioner's report of 1986. Under the previous IOCA legislation's corresponding but more limiting section, such "internal targeting" by GCHQ was allowed **only for counter-terror** purposes. He therefore invented a non-statutory procedure to make this lawful for other purposes which he called an "overlapping warrant". This was a domestic warrant made out for the targeted person's (both internal and external) communications.

31. Intentionally or otherwise, in doing so Lord Lloyd elided the problem that GCHQ might only have discovered the identity of the person they wished to target inside the UK, through mass-surveillance of external communications by some other (non-personal) "factor". In this way a person inside the UK could fall under much more intensive surveillance through the fruit of the poisoned tree of GCHQ "external" mass-surveillance. To this problem, Lord Bassam replied[22] to questions in the RIPA debates that "*it would of course be unlawful to **seek** to catch internal communications in the absence of an overlapping warrant or a certificate complying with*" section 16. In this way, RIPA s.16 facially legitimated a huge (if little appreciated) extension of GCHQ's domestic surveillance power, beyond counter-terrorism, for the full range of interception purposes.

32. This example of s.16 is offered to illustrate how redrafting RIPA and closing the gap between the public understanding of surveillance powers and the reality is no simple matter, given a history of deceptive drafting and enactment with some degree of long-standing complicity by party leaderships not to delve into these matters in Parliament.

33. Some proposals for specific reforms were included in my submission to the CDB Joint Committee in 2012[23]. Further suggestions may be offered in oral evidence to the ISC.

February 2014

[21] Paras 33-36, 1986/87 Cm 108 *Interception of Communications Act 1985. Chapter 56. Report of the commissioner for 1986* https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/iocc/IoCC%201986.pdf

[22] Lord Bassam of Brighton to Lord Phillips of Sudbury, 4th July 2000, *re: RIP Bill Committee: Clause 15* http://www.fipr.org/rip/Bassam%20reply%20to%20Phillips%20on%20S.15.3.htm

[23] ibid.

Caspar Bowden

Submission to the Joint Committee on the draft Communications Data Bill

Caspar Bowden is an independent advocate for information privacy rights. He was an expert adviser to Opposition parties in the House of Lords for five bills[1], and author of the first paper on communications data retention[2] and the most comprehensive online resource on RIPA[3]. From 2002-2011 he was Chief Privacy Adviser to Microsoft in 40 countries, and from 1998-2002 was Director of the Foundation for Information Policy Research (www.fipr.org). He is a specialist in Data Protection policy, EU and US surveillance law, privacy research in computer science, and a fellow of the British Computer Society. He advises several civil society associations, and sits as an independent expert on the EU Committee for implementing the Data Retention Directive[4]. The opinions in this submission are the author's own and do not represent any organization.

1 RIPA 2000, H&SCA 2001, ATCSA 2001, ID Cards Acts 2005/6

2 "CCTV for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation", Caspar Bowden, Computer and Telecommunications Law Review 2002 (http://scholarship.law.duke.edu/dltr/vol1/iss1/47/)

3 Information Centre for the Regulation of Investigatory Powers Act (www.fipr.org/rip/)

4 Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime (http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2230)

Summary and recommendations

"The Data Retention Directive is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects" - Peter Hustinx[5], European Data Protection Supervisor

The Communications Data Bill[6] is the most dangerous long-term threat to a free society ever proposed by a democratic government, and should be rejected in its entirety. This response is lengthy to provide historical and policy context to the Joint Committee[7] integrating knowledge from several disciplines.

Over two decades the UK has been in the vanguard[8] of a core group of five European countries[9] seeking systematic Internet surveillance. A blanket *retention* regime gives law-enforcement an "Internet Tardis" to go back in time and find out retrospectively what anyone was thinking about, who they were talking to, and where they were. A *preservation* regime is opposed by security bureaucracies because they would be obliged to seek authorization case- by-case (and they might be held to account for those decisions retrospectively).

No official scheme for preservation has ever been published. The author has consistently advocated for data preservation as the only viable alternative policy to retention, and the following summary proposals develop a position first outlined eleven years ago, which respects human rights, with proportionate and effective means for law-enforcement:

- Quick-response preservation on persons who have been identified as facing a real and immediate serious threat, and designated vulnerable groups.
- Convicts of specified crimes released on license must register their means of electronic communication for data preservation during a prescribed period.
- Case-by-case judicial authorization for preservation, targeted at those reasonably believed to be engaged in criminal activities (with emergency procedures). Similar reforms should be made for prior judicial approval of interception warrants. Targets should be notified afterwards of preservation and/or interception where suspicions prove unfounded (unless there are compelling reasons not to do so).
- A centre for analysis of preserved data, intended to investigate links between criminal groups, and generate new targets for preservation (subject to judicial authorization)
- Replace the current three Commissioners with a unified Surveillance Commission, reporting to Parliament, with multi-skilled investigators including human rights and computer experts, credibly able to detect and deter abuse, corruption, and insider attacks.
- A fixed ceiling on the number of interception warrants, and a larger ceiling for targets of communications data preservation, which could only be altered by Parliament.

5 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeche s/2010/10-12-03_Data_retention_speech_PH_EN.pdf

6 Draft Communications Data Bill 14th June 2012 http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf

7 http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/

8 Duncan Campbell 28.06.1999, Britain Sneaks "Enfopol" Plan Into Action, (http://www.heise.de/tp/artikel/2/2989/1.html alsohttp://www.heise.de/tp/artikel/6/6398/1.html)

9 UK, Germany, France, the Netherlands, Sweden

The dichotomy of data retention versus data preservation

"There was something called liberalism. Parliament, if you know what that was, passed a law against it. The records survive. Speeches about liberty of the subject."

Brave New World 1932, Aldous Huxley (and biographer of Père Joseph, Richelieu's eminence gris)

The policy choice between data retention and preservation is a sharp dichotomy. Either data exists or it doesn't. The main objections of principle to mandatory systematic retention of communications data are:

- a "time machine" to scrutinize everyone's past behaviour without prior reason is tyrannical
- Internet and mobile usage patterns reveal sensitive data about e.g. politics and intimate life
- mass-surveillance of every online social relationship is incompatible with a free society
- location data has special privacy risks because it can easily be correlated with other data
- claims that it is necessary just to "maintain police capabilities" don't stand up to scrutiny
- communications data may be equally (or more) intrusive than interception of content
- most criminals could be caught by targeted data preservation rather than blanket retention
- data retention has only happened through rushed legislation in response to shocking events
- if retention of communications data is justifiable, why not every other kind of data also?

Proponents of data retention often say they cannot understand the reasons of objectors. They say that the data will only be accessed with proper authority when justifiable; obviously circumstances exist in which no amount of foresight can guarantee that useful data will have been preserved. UK public opinion has never registered strong objections (unlike e.g. Germany which has seen protests in 40 cities[10]), and the police insist the data is vital. So why object?

The essential reason is that although public opinion does not seem today any more concerned about the intensification of surveillance capabilities using "traffic analysis", "data-mining", "social network analysis", that is a very short term view. Ubiquitous personal communication technologies are here to stay, and because of exponentially falling data storage costs, in the long run two contrasting states of society can be envisaged. Subject to exceptions, the default must be either that individuals determine whether and when their history is recorded, or data will exist about everyone all the time. At some point in the future, most people *will* understand the reality of "dataveillance"[11] and the loss of associated freedoms. UK policy is based on the idea that so long as this doesn't happen there is "no chilling effect, no problem" for democracy.

Another argument often heard from government is "Google/Tesco envy" - what about the mountains of data (more or less) lawfully accumulated in the private sector? Why should the state not also collect "Big Data" and use for socially beneficial purposes? The weight of disinterested opinion amongst information privacy and security experts is clear.
Indiscriminate accumulation of personal data is storing up trouble and the vaunted benefits of Big Data often amount to exploitation without compensation, which will likely have socially regressive[12] outcomes. Intense commercial lobbying is already underway to deflect and dilute regulation which could prevent these harms.

10 http://www.vorratsdatenspeicherung.de/content/view/161/79/lang,en/
11 http://www.rogerclarke.com/DV/
12 e.g. behavioural advertising will discriminate against the least affluent, least able to participate in commercial life

New computer science research shows how "privacy engineering"[13] can maintain the autonomy and discretion we depend on to explore new social and personal experiences, seek medical treatment and spiritual advice, and enable journalists to research confidentially what it would be impolitic to report with attribution. However data retention and the slow pace of legal reform is rapidly demolishing most traditional possibilities for such privileged professional and political privacy. Even in the US, with the Constitutional primacy given to freedom of expression and indemnities to the press [14]

Reporters Committee for Freedom of the Press, an advocacy group, said the effect of the current investigation comes on top of a growing awareness by journalists in the last two years that the government often tracks employees' e-mail and telephone contacts. "Reporters are beginning to resort to the old practice of meeting on a park bench to avoid leaving an electronic trail"

From Data Retention to data-mining

"The biggest problem is that Member States use retention today not only to combat terrorism and serious crime. After the so-called e-Privacy Directive, such data may be used for other purposes, such as crime prevention or the protection of public order, which is a very vague term... The application must be strictly limited to terrorism and serious crime." EU Commissioner Celia Malmström[15] 7th July 2012

Communications data retention is a policy made in Britain.

The lineage of traffic analysis (analysis of patterns of communications about who-is-talking- to-whom) as an intelligence technique can be traced back to WW2 and even WW1.[16]

In 1991 an ITV documentary on electronic surveillance included an interview with a former Joint Intelligence Committee official[17], who disclosed the existence of a memorandum from Sir Peter Marychurch (Director of GCHQ) which seems to have suggested the data-mining of domestic communications data for security purposes.

Police, security and intelligence organizations have been seeking to establish mandatory systematic data retention since at least 2000. An unpublished paper[18] from the major UK Agencies collectively lobbying the Home Office to introduce a "National Data Warehouse" was posted on the Internet and is worth re-reading for its precocious ambition.

4. WHAT TYPE OF DATA SHOULD BE RETAINED? ..**All** communications data generated in the course of a CSP's business **or routed through their network or servers,** involving both Internet and telephone services, within a **widely interpreted** definition of "communications data"

6.1.1 ...The Agencies' position is, therefore, that data should be retained for **FIVE YEARS**

13 Digital Privacy: Theory, Technologies and Practices. Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis, Costas Lambrinoudakis (eds). Auerbach Publications (Taylor and Francis Group), 2007

14 New York Times 1st August 2012 "Inquiry Into U.S. Leaks Is Casting Chill Over Coverage" (http://www.nytimes.com/2012/08/02/us/national-security-leaks-lead-to-fbi-hunt-and-news-chill.html?_r=2&pagewanted=all&pagewanted=print)

15 http://www.faz.net/aktuell/politik/europaeische-union/eu-innenkommissarin-cecilia-malmstroem-wir-waren-sehr-geduldig-mit-deutschland-11808962.html

16 George Danezis , Richard Clayton, Introducing Traffic Analysis (2007) (http://research.microsoft.com/en-us/um/people/gdane/papers/TAIntro-book.pdf)

17 ITV World in Action 1991, "Defending the Realm", Nick Davies interviewing Robin Robison (former JIC official)

18 "Looking To The Future" submission to the Home Office for legislation on data retention from ACPO, ACPO(S), HMC&E, SS, SIS, GCHQ (21st August 2000) - (http://cryptome.org/ncis-carnivore.htm)

6.6.4 If the figures are expanded to try and establish the global cost of data storage and retrieval across the UK market, it is estimated to amount to around **£9 million per annum**

The kernel of the CDB was already fully formed in 2000, before the Olympics, national scale rioting, 7/7, Iraq, Afghanistan, and 9/11. There is the difference of a still staggering demand for a longer retention period than has ever been contemplated in any country[19], the estimated costs are now twenty times higher[20] (£1.8bn over 10 years), and the agenda of generalized data-mining is now (more or less) out in the open, albeit euphemistically dubbed "Filtering" (of humongous amounts of data which ought not to be created for retention in the first place except in some rickety 60's TV dystopia).

Bowden's 2002 paper on data retention went to press before ACTSA 2001 passed, but stated

> Automated trawling of traffic databases is a powerful form of mass-surveillance over the associations and relationships that constitute private life. It also reveals the sequence and pattern of thought of individuals using the Internet – it could be described as "closed circuit television for the inside of your head"
>
> ...At the same time (NCIS) were lobbying in secret to warehouse the entire population's traffic data, the Director of NCIS wrote that "conspiracy theorists must not be allowed to get away with the ridiculous notion that law enforcement would or even could monitor all emails."[21]

One of the major purposes of traffic analysis of communications data is to identify targets through pattern analysis. The DG for counter-terrorism at the Home Office asserted in evidence to the Draft CDB Committee that

> Charles Farr[22] (Q28): If you have the data provided for in this legislation, then you can resolve increasingly anonymous communications, which are a feature of the communications environment in which we live. To put it another way, if you have the right kind of data, issues of anonymisation cease to be a significant problem.

9/11 and "Warrantless Wiretapping" in the US

In a different forum, three days later, a senior technical expert who designed very large-scale traffic analysis systems for the National Security Agency (the US counterpart to GCHQ) explained how, on the contrary, mobile telephone anonymity could always be maintained with elementary tradecraft

William Binney[23]: "buy throwaway phones and keep buying them...the most secure way is for you to buy two phones, give one to your friend and you take one, it will show up in the graph as a link, an isolated link, but you'll not be connected anywhere"

It seems unlikely that such a simple counter-measure would not be well understood by terrorists, even if traffic analysis would be effective against opportunistic perpetrators of less serious crimes.

Mr. Binney became a whistleblower because he was concerned that the NSA was spying on

19 except for Poland, which legislated 8 years briefly by accident in the mid 00's, and then swiftly repealed

20 http://www.computerworlduk.com/news/it-business/3364147/governments-data-snooping-bill-will-cost- 18bn/

21 http://www.guardian.co.uk/technology/2000/jun/15/security.internet

22 Uncorrected Oral Evidence Taken Before The Joint Committee On The Draft Communications Data Bill (10th July2012)-http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf

23 Keynote at HOPE 9 conf (New York City, 13th July 2012, http://www.youtube.lu/watch?v=hqN59beaFMI 1hr 12m)

Americans illegally using traffic analysis of communications data, very much as is being proposed in the "Request Filtering" Clause 14 of the UK draft CDB bill. In his remarkable speech, worth watching in its entirety, he describes how the NSA had already sought such data illegally in February 2001[24] (i.e. before 9/11 and the passage of the notorious Patriot Act). After 9/11, the NSA initiated several further communications mass-surveillance activities which became known collectively as "warrantless wiretapping" including one codenamed *Stellar Wind*. These programs only came to light as a result of diligent investigative reporting using information provided by NSA (and FBI) whistleblowers concerned about violations of the US Constitution and statute law. For several years, these whistleblowers (and journalists and editors) have been threatened with prosecution on specious charges. Although still not widely reported, a consistent pattern to have emerged is that official channels for escalation, investigation and Congressional scrutiny were thwarted with the complicity of some of the most senior legislative and judicial authorities. Only after the revelations of New York Times journalists James Risen and Erich Lichtblau were published in 2005 (after their newspaper censored itself for a year until after the 2004 election) did a complaisant Congress "make what had been illegal, legal" (in the words of another NSA whistleblower Thomas Drake[25]) through passing the Protect America Act 2007 and the FISA Amendment Act 2008.

RIPA s.16(3) – (effectively) "Warrantless Wiretapping" inside the UK?

The relevance of all the above to the UK is that in an almost unnoticed section of RIPA 2000, the same issue had been anticipated and legalized pre-emptively. There was substantial debate on this point in the House of Lords as a result of amendments and briefing[26] from the Foundation for Information Policy Research. Lord Bassam responded to points in debate in a letter[27] to Lord Phillips of Sudbury

> **Lord Bassam**: ....in some cases selection (of traffic for mass surveillance) 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 [Section 16(3)]

Although the front-benches then played down the issue (as a result of briefing from GCHQ), some back-benchers remained dissatisfied at Report[28]stage

> **Lord Lucas**: Both (front-bench) noble Lords seemed to be striving extremely hard to give the Government the benefit of the doubt and to find some way in which what is written plainly and clearly in the Bill should not be true. It is absolutely obvious what is in the Bill--at least it is to me--and that is, yes, trawling becomes legal. The Home Secretary has to renew the warrant every three months, but he can trawl on grounds of economic well-being and serious crime, as well as terrorism, to any extent that he wishes.

By analogy, two US senators[29] have recently blocked renewal of the corresponding 2008 law

24 ibid 32m

25 DemocracyNow interview with Thomas Drake 26th March 2012 http://www.democracynow.org/2012/3/26/part_2_former_nsa_employee_thomas 49m

26 http://www.fipr.org/rip/#Overlapping

27 http://www.fipr.org/rip/Bassam%20reply%20to%20Phillips%20on%20S.15.3.htm

28 Lords Hansard 12th July 2000 – http://hansard.millbanksystems.com/lords/2000/jul/12/regulation-of-investigatory-powers-bull#S5LV0615P0_20000712_HOL_383

29 http://www.wyden.senate.gov/news/press-releases/wyden-places-hold-on-fisa-amendments-act-extension

because

> (they asked for) an estimate of the "number of people located in the United States whose communications were reviewed by the government pursuant to the FISA Amendments Act." The Office of the Director of National Intelligence responded that it was "not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the authority of the FAA."

However the analogy between the controversy over RIPA 2000 s.16(3) and the FISA Amendment Act 2008 s.1881a does not hold in four important senses. Firstly, the controversy in the US has been documented in books[30], magazines[31] [32], newspapers[33], current affairs television programs[34] and websites[35] (although it remains little understood in the legislature) as a result of insider whistleblowers concerned that the categorical protections promised to US citizens by statutes and the Constitution were being illegally subverted.

In contrast in the UK, the issues arising from RIPA 16(3) have only been considered (outside of government) by a few members of the House of Lords and a handful of surveillance policy analysts (and never by a Parliamentary Select Committee, or the Intelligence and Security Committee, POST, or the Investigatory Powers Tribunal – unless perhaps in secret). There has been exactly one press article[36], and no books or television discussion whatsoever.

A second difference from the US situation is that the UK statutes do not promise any analogous categorically superior protections to UK citizens, indeed they cannot do so because discriminating by nationality in this way would be incompatible with the Human Rights Act[37]. Instead RIPA defines *external* communications as those which begin or end outside the UK, and "certificated" warrants for trawling through these using super-computers to search for abstract "factors"[38]. The Bassam letter reveals the government in 2000 well-understood that the *external* concept was incoherent for digital communications using multi-layered protocols, split into datagrams, and autonomously routed through packet-switched networks. However this issue was far ahead of what Parliament could then assimilate, so there was no proper deliberation of the consequences for privacy and freedom, in the way that is now happening – to some extent – in the US. The comparison between the UK and the US is especially relevant because of the longstanding intelligence ties between NSA and GCHQ, and their Internet surveillance capabilities are much larger than all other democratic countries.

Thirdly, whilst the intentional warrantless mass-surveillance documented in the US has been widely criticized as illegal, we do not know if any analogous domestic mass-surveillance has

---

30 Erich Lichtblau "Bush's Law: The Remaking of American Justice", 2008, Pantheon

31 Jane Mayer, The New Yorker "The Secret Sharer" (http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all) 23rd May 2011

32 James Bamford, Wired "The NSA Is Building the Country's Biggest Spy Center" 15th March 2012 (http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/)

33 Siobbhan Gorman, Wall Street Journal "NSA's Domestic Spying Grows As Agency Sweeps Up Data" (http://online.wsj.com/article/SB120511973377523845.html) 10th March 2008

34 PBS "The Spy Factory" 3rd February 2009 (http://www.pbs.org/wgbh/nova/military/spy-factory.htm)

35 http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy

36 The author attempted to brief newspaper and broadcast current affairs editors without any apparent interest, resulting in only in http://www.guardian.co.uk/technology/2000/aug/10/news.onlinesupplement

37 A v. Secretary State Home Department [2004] UKHL 56, [2005] 2 AC 68

38 Factors may select according to traffic patterns (who-is-talking-to-whom), keywords, voiceprints, and algorithms also exist for searching texts for paraphrased meaning ("latent semantic indexing")

been authorized under RIPA S.16(3) certificated warrants. The Interception Commissioner has never referred to that section in his published annual reports, or indeed made any reference to "certificated" (trawling) warrants[39]. Interpretation of the 16(3) clause requires unraveling nested and interlocking clauses, phrased in triple-negatives using pseudo-technical jargon. No open jurisprudence or scholarship can develop because of the secrecy provisions of RIPA. The UK lost a relevant case at the ECtHR in Strasbourg in 2008[40] but that concerned the previous IOCA 1985 law. The Bassam letter is all that is known, but we do not even know if the IoCC is aware of that letter, agrees with or enforces its prohibitions, or understands its technicalities.

Fourthly, there are some indication[41] [42] [43]that the *Stellar Wind* program in the US mainly or wholly concerned data-mining analysis of "non content metadata" (such as communications data but perhaps other kinds of transactional records also), not mass-interception of the *contents* of communications. The distinction is habitually muddled in (every country's) press coverage and legislative debate, but traffic analysis is the primary technique for selecting what "content" gets intercepted in both targeted and mass-surveillance of communications. It might explain the blasé confidence of US administration officials that this type of data- mining did not break the FISA law – at least not in the way most critics alleged.

However the privacy-invasive reality of traffic analysis in bulk is not adequately recognized in US or UK law. The post-9/11 surveillance-industrial complex is founded on the shibboleth that whilst "content" deserves the protection of a warrant, "mere" communications data engages privacy rights to a vastly lesser extent, and its acquisition may be self-authorized by law enforcement agencies. This legal fiction is precariously sustained by law enforcement agencies carefully avoiding test cases which might update binding precedents dating from the era of mechanical telephone exchanges[44].

The Anti-Terrorism Crime and Security Act 2001 Ch.11 introduced a power to compel blanket retention of communications data, if service providers declined to do so "voluntarily". The Liberal Democrats introduced an amendment which sought instead only to permit preservation of data "directly or indirectly related to national security"[45].

> Lord Phillips of Sudbury: ...whatever the Minister thinks about mass trawling and mass surveillance, the Home Office knows that that is precisely what these clauses relate to. It is their ability, via the Secretary of State's direction, to require the entire industry to retain its entire stock of traffic data for an unlimited period. It is that power that enables the security industry to have access, via the Regulation of Investigatory Powers Act and the Data Protection Act, to this huge warehouse of information. We on this side of the House have repeatedly said that we are not content with the balance as struck. That is why we want the amendment to remain.

39 Except in the first report which dubiously invented "overlapping" warrants http://www.fipr.org/rip/#Overlapping

40 Liberty and others v UK no. 58243/00 [2008] ECHR

41 http://en.wikipedia.org/wiki/NSA_call_database

42 US wiretap law authority Orin Kerr on 15th December 2008 (http://www.volokh.com/posts/1229325134.shtml)

43 Newsweek 12th Dec 2008 (http://www.thedailybeast.com/newsweek/2008/12/13/now-we-know-what-the-battle-was-about.html)

44 Tokson M, Automation and the Fourth Amendment, Iowa Law Review, 2011 (http://128.255.56.99/~ilr/issues/ILR_96-2_Tokson.pdf)

45 Lords Hansard 13th Dec 2001 (http://www.publications.parliament.uk/pa/ld200102/ldhansrd/vo011213/text/11213-17.htm)

> ...NCIS is building—and has made it quite clear that it wants to go on building—a national traffic data warehouse. That is its aim. Indeed, a senior member of that body said recently, "We want to have all the information we can lay hands on. It's up to you fellows to stop us".

In an exhausting debate between both Houses, in which few parliamentarians grasped the conceptual difference between retaining data on the entire population versus the small fraction about whom prior suspicions might exist, the amendment was only accepted by the government in a fog of confusion with a seemingly incoherent rationale[46]. A QC's Opinion[47] later obtained by the Information Commissioner found that blanket retention was "a breach of the right to privacy", anticipating subsequent arguments over the EU Data Retention Directive[48], but the ICO chose to acquiesce to the Home Office and offered no further resistance.

Waiting for Strasbourg (or Luxembourg) ?

Several Constitutional Courts around Europe have ruled that blanket data retention is unlawful[49]. A case initiated by Digital Rights Ireland which will test the human rights compatibility of the DR Directive is now in progress at the ECJ[50]. The ECtHR has recognized in unambiguous judgments[51] that the right to private life under Article 8 is engaged by (a) processing communications data per se, or (b) the "mere" *collection* of data about individuals (irrespective of whether it is examined), or (c) the indiscriminate accumulation of data about entire populations. Putting a/b/c together, logically the Court ought to find (when a suitable case arrives) that the principle of blanket retention of communications data for the purposes of traffic-analysis through data-mining is at least a disproportionate violation of Art.8, and perhaps also that not only is this unnecessary in a democratic society, it is incompatible with democracy. This conclusion can also be deduced from the General Comment on the right to privacy in International Covenant of Civil and Political Rights[52].

> Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use

---

46 Commons Hansard 13th Dec 2001, David Blunkett (Home Secretary): "The amendment, in relation to part 11 therefore suggests that we should try to separate out those parts of data. As I tried to explain on a number of occasions, including last night, it is not possible to do that, but **paradoxically, because it is not possible to do it, it is not reasonable to suggest that we should not do it**. I am therefore prepared to accept the amendments that have been tabled. **In order to be able to implement what they want, we will have to retain the data**, so that it can be accessed to test out whether the intelligence services are right in believing that it is relevant in tackling terrorists. That is how stupid the Liberal Democrats are." (!?) (http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011213/debtext/11213-36.htm)

47 Ben Emmerson QC (31st July 2002 - http://www.guardian.co.uk/technology/2002/jul/31/internet.politics)

48 Kosta Eleni, Valcke Peggy (2006) "Retaining the data retention directive", Comp Law & Sec Report, Vol 22, Issue 5, p.370-380 http://www.law.kuleuven.be/icri/publications/824a2_Kosta,Valcke_2006_CLS_DataRetentionDirective.pdf

49 e.g. Romania which found that "a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear" http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding- data-retention.html

50 Case C-293/12 http://curia.europa.eu/juris/fiche.jsf?id=C;293;12;RP;1;P;1;C2012/0293/P

51 *ECHR (a) Malone v. UK (1984) and Copland v. UK (2007), (b) Amann v. Switzerland (2000) and Rotaru v. Romania (2000), (c) S and Marper v. UK (2008)*

52 CCRP General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) : . 04/08/1998 (http://www.unhchr.ch/tbs/doc.nsf/%28Symbol%29/23378a8724595410c12563ed004aeecd?Opendocument)

of such authorized interference must be made only by the authority designated under the law, and on a ***case-by-case basis***.

However US and ECHR jurisprudence diverge fundamentally over the privacy sensitivity of communications data. US courts have held so far that individuals have no expectation of privacy in traffic and location data because they are necessarily divulged to "third-party"[53] service operators. The UK tried out a similar argument at Strasbourg in Copland v UK[54] 2007

> UK: Although there had been some monitoring of the applicant's telephone calls, e-mails and Internet usage …this did not extend to the interception of telephone calls or the analysis of the content of websites visited by her. The monitoring thus amounted to nothing more than the analysis of automatically generated information … which, of itself, did not constitute a failure to respect private life or correspondence

The ECtHR completely rejected this view in their judgment

> 43. The Court recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone" (see *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, § 84). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1 (see *Amann*, cited above, § 65). Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings.
>
> 44. Accordingly, the Court considers that **the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and INTERNET usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8**. (emphasis added)

One of the most thorough recent examinations of the legality of the EU Retention Directive emphasized that in any determination of the compatibility of the principle of retention[55] "the fact that traffic analysis and data mining can be realistically performed using the retained traffic and location data is an aggravating factor to be considered."

A Finnish Red Herring

The Explanatory Notes of the draft CDB floats a specious compliance argument at footnote (2)

> See e.g., K.U. v Finland [2008] ECHR 2872/02, at para. 49 ("....Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. ...It is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.")

---

53 American Bar Association Journal "The Data Question: Should the Third-Party Records Doctrine Be Revisited?" (http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/) 1st August 2012

54 http://www.bailii.org/eu/cases/ECHR/2007/253.html

55 Feiler, L., "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", European Journal of Law and Technology, Vol. 1, Issue 3, 2010. (http://ejlt.org//article/view/29/75)

K.U. v Finland appeared around the time of Marper, but attracted little comment or analysis at the time in comparison, and the prominence given to it by the Home Office shows they think it is their best riposte to ECtHR's deprecation of indiscriminate collection.

But despite the (uncharacteristic) rhetorical sideswipes at Internet anonymity, it is much weaker than it seems because these remarks were in *dicta.* It is not entirely clear whether the author of the judgment understood the point, but it was not necessary in this case to consider the justifiability of blanket and indiscriminate retention of data which would not otherwise exist. The data at issue in the K.U. case did exist, but Finnish law was defective in not allowing its use to investigate the crime. It is not reasonable to assume that the ECtHR would wish to finesse such a massively important question, so the case cannot bear the the significance the Home Office implies.

Interactions with Data Protection law

"We should select any person from the inhabitants of the Earth...using no more than five individuals...he could contact the selected individual using nothing except the network of personal acquaintances" - Frigyes Karinthy[56] 1929

Communications data, even without any information about the content of communication, can reveal highly sensitive information in surprising ways. Much information is revealed through the *social graph* of relationships between individuals, particularly if each connection is annotated with strength information, such as how often two individuals communicate.

Inferring "sensitive data" from the social graph[57].

For example, introverts might communicate more often with a smaller circle of contacts who are all related, while extroverts might tend to communicate less often but with a larger circle of contacts from different social spheres, revealing a basic profile of personality. Such information can be revealed simply through patterns of communication, which sociologists have studied for decades prior to the advent of widespread Internet communication[58].

Much more powerful inferences can be drawn using the principle of *homophily* - most people are much more likely to communicate frequently with individuals who are like them. It is a robust phenomenon and has been observed across cultures and a large number of personal traits, including age, occupation, social class, religion, political affiliation, gender and sexual orientation, and also including implicit traits like intelligence, attitudes, values, and aspirations[59].

In these ways, social network analysis of communications data can generate sensitive (aka "special category") personal data, without any knowledge of the content of communications. Data Protection Authorities have remained silent about this problem (it has scarcely been addressed in any Art.29 Opinion[60]), perhaps because it seems too corrosive to a definable

56 originator of the postulate of "six degrees of separation"

57 I am grateful to Joseph Bonneau for help with this passage

58 Wasserman, S. & Faust, K., Social Network Analysis, Cambridge University Press, 1994

59 McPherson, M., Smith-Lovin, L. & Cook, J., Birds of a feather: Homophily in social networks, Annual Review Of Sociology, Annual Reviews, {2001}, Vol. {27}, pp. {415-444}

60 Art.29 2010 WP 171 on online behavioural advertising "if an ad network provider processes individual behaviour in order to 'place him/her' in an interest category indicating a particular sexual preference they

concept of sensitive personal data.

With the advent of online social networks, researchers have recently been able to acquire sufficiently large datasets to demonstrate the power of large-scale inference using homophily. Given information about private traits of some individuals, such as sexual orientation or religion, it is possible accurately to predict this trait for many other individuals using the social graph.[61] Very similar experiments have successfully demonstrated prediction of users' political affiliation[62] [63] [64], gender[65] [66], and hobbies[67]. This type of inference could improve significantly given a more fine-grained social graph with information about the frequency and duration of communication between individuals.

Limits to the scope of communications data – Big Browser

"If you give me six lines written by the most honest man, I will find something in them to hang him" - Cardinal Richelieu (1585-1642)

The definition of communications data in the draft CDB are essentially unchanged from RIPA 2000. The definition included the name (or IP address) of web-sites browsed (www.bbc.co.uk), but excludes anything "after the first slash" (www.bbc.co.uk**/news/uk-politics-18003315**).

It is worth recalling the sequence of events which resulted in this limitation. During the RIPA debate in the House of Commons, FIPR warned[68] that any logs of web-pages visited (in the transparent caches of an ISP or logs retained by hybrid communication services incorporating search engines or portals) could be caught in the vague definitions, and promoted amendments to draw out the government's position in the House of Lords. A quickening tempo of adverse media coverage[69] in the trade and broadsheet press increased the pressure for changes and clarifications which had been impassively blocked for many months previously

Lord Lucas: ...the identity of every single web page that is visited is known. It is as if

would be processing sensitive data"

61 This approach was famously demonstrated in the case of sexual orientation, where a very simple algorithm using only binary friendship connection information and a small number of men known to be homosexual was sufficient to predict the sexual orientation of about 6,000 students at MIT with about 80% accuracy

62 Lindamood, J., Heatherly, R., Kantarcioglu, M. & Thuraisingham, B. Inferring private information using social network data, Proceedings of the 18th International Conference on World Wide Web, ACM, 2009, pp. 1145-1146

63 Mislove, A., Viswanath, B., Gummadi, K.P. & Druschel, P. You are who you know: inferring user profiles in online social networks, Proceedings of the Third ACM International Conference on Web Search and Data Mining ACM, 2010, pp. 251-260

64 Zheleva, E. & Getoor, L. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles, Proceedings of the 18th International Conference on World Wide Web, ACM, 2009, pp. 531-540

65 Kozikowski, P. & Groh, G. Inferring Profile Elements from Publicly Available Social Network Data 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust 2011, pp. 876-881

66 Xu, W., Zhou, X. & Li, L. Inferring privacy information via social relations, Data Engineering Workshop, 2008. ICDEW 2008. IEEE 24th International Conference on 2008, pp. 525-530

67 Agarwal, A., Rambow, O. & Bhardwaj, N. Predicting Interests of People on Online Social Networks, CSE '09: International Conference on Computational Science and Engineering

68 FIPR Press Release on RIP Third Reading HoC debate 9th May 2000 http://www.fipr.org/rip/PR3RHC.htm

69 http://www.fipr.org/rip/#Observer250600

> under the heading "communications data" the Government are able to know about every shop that I have visited and every page of every book, magazine or article I have read. If I make a request to a search engine, in most formats that counts as communications data because it is a signal to actuate the search engine.
>
> Lord Cope of Berkeley: ..."communications data" on the Internet widens the issue a great deal, in particular, in relation to visits to websites, and so on. ... We believe that it may be necessary to have greater controls over the extent of this intrusion than at present.
>
> Lord Bassam: It is becoming clear that the current definition is not adequate... I do not have a new definition of "communications data" to offer today

The mini-debate[70] shows the House of Lords at its zenith as a revising chamber, but its powers to convert forensic cross-examination into textual changes were (and are) rather modest. The critical factor was a general loss of confidence in the Executive's competence about the subject's technicalities, which obliged the Bill team to make unusually sweeping revisions to these and other sections, under an intense degree of press scrutiny[71] to "keep them honest", resulting in the definitions we have today for *Subscriber*, *Traffic* and *Use* data[72].

Police requests to access *Subscriber* data (for account billing) have never needed judicial authorization, but this category inaptly includes device serial numbers which can track behavior. *Traffic* data is the most privacy-sensitive (who-is-talking-to-what-or-whom) which also includes location data (GPS coordinates or mobile base-station IDs). However despite the hard-won Big Browser amendment, a technique involving *Use* data means **content** could still be deduced through "fingerprinting"[73] the pages of websites.

This loophole should be closed as part of a new concept of regulating the *mode of analysis* for human rights compliance (see below), but it will need Commissioners with technical as well as legal expertise to apply (see below on IoCC oversight)**.**

The problem of schizoid-jurisdiction

A problem which has developed in the past decade is that some providers of Internet services with headquarters in the US have developed the practice of rejecting the application of EU jurisdiction for purposes of Data Protection (for example relying on Safe Harbor for minimal fulfillment of the rights of the data subject), but on the other hand they will respond locally and directly to demands from law enforcement authorities for access to communications data (without insisting on the analogous step of requiring LEAs to invoke MLAT procedures). There is no legal basis for such a schizoid attitude to recognizing jurisdiction, and this practice only continues because (a) the organizational functions for data privacy are often disconnected from the servicing of law enforcement requests, and (b) some DPAs and even the Council of Europe may be aware of these practices but find it expedient to turn a blind eye absent a sharp test of data subject rights. Nevertheless, personal data are being processed within the EU when law enforcement demands are serviced in this way and data subjects are entitled to full exercise of their rights against the Controller within EU jurisdiction.

---

70 http://hansard.millbanksystems.com/lords/2000/jun/19/regulation-of-investigatory-powers-bill-2#S5LV0614P0_20000619_HOL_458

71 The author briefed more than 100 journalists over a 12 month period from 1999 until Royal Assent

72 Draft CDB Clause 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.

73 https://blog.torproject.org/blog/experimental-defense-website-traffic-fingerprinting

It is totally unclear how foreign service providers outside the UK (or the EU) are going to be required to comply with the provisions of the CDB, but there is clearly the risk that the problem of schizoid jurisdiction, and lack of full, prompt and effective enforceability of rights could be further aggravated.

Subject access rights to "third party" communications data ?

> ***Explanatory Notes Clause 5: Access to data***
>
> 30. Subsection (1) stipulates that communications data held by a telecommunications operator under Part 1 can only be accessed in accordance with the provisions in Part 2 or as otherwise authorised in law. *These may include a request under section 7 of the Data Protection Act 1998 (which provides an individual with the right of access to personal data)* or in pursuance of a court order.

This clause ostensibly ensures a Data Protection right of subject access (which was not expressly included in the corresponding section of RIPA Pt.1 Ch.2), and thus ought to be welcome in principle. However it is actually a bear-trap, which could mean that most of the new data collected would be ineligible for subject access.

The major purpose of CDB is blanket collection of metadata about use of "3rd party services" (e.g. those not operated by the user's ISP), to be collected by Deep Packet Inspection (DPI) boxes located throughout the UK network infrastructure (not necessarily just the retail operator with whom the user has a billing relationship). The owner of the DPI box (or the Clause 1 apparatus) will be the putative Data Controller for purposes of subject access, but they may not know (directly or indirectly) the identity of the person whose data is being collected. Because the DPA 1998 did not give any effect to four crucial words of Recital 26 ("or by any other person") of the EU DP Directive, data is only regarded as personal in the UK if it is directly identifiable by the Controller, together with other information that is or may likely come to be in the Controller's possession. Therefore the Controller will be entitled to refuse access to any data which it cannot exclusively and directly associate with the subject. This might include any data possibly being relayed by the user on behalf of another party (e.g. peer-to-peer routing protocols such as Skype[74]). The position is not even clear for the user's direct communications with another party. The ISP only knows the association between the user's IP address and subscriber account details; it does not "know" about the user's identifiers and handles at other protocol levels of abstraction (but the ISP will nevertheless be obliged to install DPI boxes which do capture metadata from these higher levels of abstraction). The Controller may even refuse to grant an access request on the grounds that the party with whom the user is communicating (if that is a natural person) has at least co-equal status as a data subject, and only agree to fulfill the request with the express consent of the other party.

Will the user be able to make a subject access request to the operator of filtering apparatus in Clause 14, namely the Secretary of State, perhaps as a putative (co-)Controller of the DPI boxes? It appears this has not been provided for in Clause 5 or elsewhere, and several DPA 1998 exemptions might be arguable, notably s.28 (national security) and/or s.29 (prevention/detection of crime). Data processed by GCHQ or for national security would be

74 See Stevens et al. "I Know Where You are and What You are Sharing" - (www.mpi-sws.org/~stevens/pubs/imc11.pdf)

categorically exempt from most parts of the DPA.

Moreover, the proposed new EU DP Regulation, which would otherwise be expected to broaden the UK concept of personal data (at last unambiguously) to include indirectly identifiable data, will not fill this lacuna if the UK's position[75] on the new Regulation in the Council of Ministers prevails. The UK wishes that only "easily identifiable" data should be considered personal (footnote 12), to delete the Recital highlighting the dangers of profiling (footnote 11), and "questioned whether so-called (online) identifiers which were never used to trace back to a data subject should also be considered as personal data" (footnote 14; see also footnote 45).

The combined effect of these UK positions on the new DP Regulation would mean that perhaps most of the captured data about 3rd party services would be ineligible for subject access, and result in a calamitous evisceration of data subject rights. The following steps would disarm this bear-trap:

(a) a right of access must be established against the Secretary of State, with explicit wording to prevent invocation of DPA s.28/29 exemptions, and

(b) a broad meaning of personal data comprehending Recital 26 of the EU DPD should be adopted (or that in the unmolested new Regulation – which already has some weasel-worded Recitals that need excision)

The effect of (a) and (b) must be for the data subject to be able to invoke the distributed data-mining machinery of (Clause.14) Filters to discover what personal data – in a broad sense – the totality of the CDB system knows about them. Any data which could be associated with the data subject as a result of a Request Filter ought to be eligible. Only in this way can the data subject be guaranteed a right of "information self-awareness" which will allow them to regulate their conduct in the sense of ECHR Art.8 quality-of-law requirements. This is a core reason for the existence of the right of subject access.

Distributed data-mining : the core of the Communications Data Bill

Although it has been touted as a concession to and measure protective of civil liberties, from a technical viewpoint it is cold comfort that the draft CDB is based on the idea of leaving data in the distributed custody of service providers, because very probably the notion of a centralized database was always going to be impractical. Few organization have experience of designing national-scale centralized data warehouses for communications data. The NSA tried with their TrailBlazer[76] project which failed expensively. NSA systems architect and whistleblower William Binney explained[77] the key problem with orthodox relational databases was that they could not ingest new data fast enough, so became backlogged. He had some success obviating this problem using fast database structures suitable for very large working memory sets, and explained that once the connections in the "national social graph" grew to a certain scale, the growth in complexity began to flatten out because already established connections began to be repeated. However collection of all the data desired by

75 www.statewatch.org/news/2012/jun/eu-council-revised-dp-position-11326-12.pdf

76 http://en.wikipedia.org/wiki/Trailblazer_Project

77 Keynote at HOPE 9 conference (New York City, 13th July 2012, http://www.youtube.lu/watch?v=hqN59beaFMI 50m).

the architects of CDB is probably out of reach even of these highly optimized techniques, and the intention is clearly to use the distributed computational technique commonly known as MapReduce[78]. Essentially this is an efficient way for applying a function to a vector of data physically distributed across many machines, bringing the intermediate results back to a central location, and then performing a final reduction of intermediate results to produce a finished massively-parallel computation.

This is what is described in Clause 14, and the explanatory memorandum reads like marketing jargon from a surveillance trade fair[79]. In fact it may be the first clause of legislation derived from a sales brochure.

> Explanatory Memorandum 82.
>
> ...The Request Filter may: a) provide **details of different options** the Request Filter may employ to provide a response to a specific public authority data request; and b) for each identified option, provide **details of the anticipated levels of interference** and the **likely precision** of the returned results. The information provided by the Request Filter will enable the designated senior officer to **understand how the Filter will answer particular questions**, and will guide him through the **process of determining which questions he believes it is necessary and proportionate to ask**, taking into account the filtering and processing which will be undertaken and the **volume of filtered data** which will be disclosed.

An amendment which removed the following highlighted parts of the "MapReduce Clause" would neutralize the capacity to do distributed data-mining (and thus prevent the system being used with capabilities equivalent to a centralized system).

> 14(2)b (i) obtaining the data **or data from which the data may be derived**,
>
> (ii) processing the data **or the data from which it may be derived** , (and **retaining data temporarily** for that purpose)

Compounding the hyper-Orwellian menace of data-mining a national traffic data warehouse (described by a former DPP[80] as a "*hellhouse* of personal and private information"), is the foreseeable risk that insiders could collude to bypass controls. Using seemingly legitimate Filters which triggered distributed queries to many DPI boxes, information about a surreptitious target could be extracted (under the rubric of "**retaining data temporarily** for that purpose"). It would be very difficult to detect or prove this was happening and the IoCC as presently operating would find nothing suspicious in the log files (assuming he was even looking).

The role of the Interception of Communications Commissioner

The 2011 report[81] of the Interception of Communications Commissioner (IoCC) is the most detailed since the first report was published in 1987. The most serious deficiency of the oversight regime is only fleetingly acknowledged – it's all (literally) a paper exercise.

> "the possibility of successful deliberate abuse is very small indeed, if **statutory channels are being used".**

78 http://en.wikipedia.org/wiki/MapReduce

79 ISS World: "Big Data Analytics and Massive IP Intercept" http://issworldtraining.com/ISS_WASH/track2.html

80 Sir Ken McDonald, 31st Dec 2008 (http://www.guardian.co.uk/uk/2008/dec/31/privacy-civil-liberties)

81 Interception of Communication Commissioner 2011 Report www.intelligencecommissioners.com/docs/0496.pdf

The reports have always been silent about how abuse by insiders with the technical or administrative ability to bypass the paperwork might be deterred or detected, yet that is surely one of the major risks.

FIPR successfully promoted a RIPA amendment[82] allowing the IoCC to insist that reliable and verifiable technical means[83] must be designed into interception and communications data logging equipment, but he has never referred in any report to exercising these powers, and it appears that efforts at verification are confined to comparing paper copies of documents held by different parties.

The IoCC always has appeared primarily to rely on those he is charged with overseeing, themselves volunteering reports of their own mistakes. Errors are lamented and usually rather trifling (typically a transposed digit). But over 27 years, the IoCC has never discovered any serious wrongdoing in interception practices whatsoever (that he has revealed publicly).

This year, for the first time, the report quantifies errors discovered by the inspection regime (rather than self-reported). However the size of the random sample (out of a half-million requests – each of which may involve data about many individuals) is not given, without which the overall number of undetected errors can only be guesstimated, but there are likely to be thousands. The IoCC has replied that it is "not possible" to give the sample size. Why not?

The report mentions that two individuals have suffered very serious consequences through such errors, but appears blind to the statistical inevitability than many more victims of such errors must be suffering equally serious injustices.

Overall the UK appears relatively secretive and compares poorly to other countries in the degree of Parliamentary involvement in the oversight process according to a comprehensive recent report to the European Parliament[84]

> In the case of oversight of information sharing, it is doubtful if the current UK arrangements satisfy the standards proposed by the UN Special Rapporteur. Domestic legislation fails to outline 'clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence'. **Nor does it explicitly prohibit the use of foreign intelligence services to circumvent national legal or institutional controls**....the UK experience underlines the **need for critical distance from the executive** to be woven into oversight arrangements (especially in such procedural questions as appointment of overseers and reporting) if public confidence is to be retained .

In contrast, under the French system a "qualified person" (with deputies) is appointed by an independent control Commission (CNCIS[85]) to conduct **prior** validation of all counter- terrorist requests for communications data, and the Commission also applies scrutiny

82 Lord Bassam's remarks on Amendment 50A 10th June 2000 (http://hansard.millbanksystems.com/lords/2000/jun/19/regulation-of-investigatory-powers-bill#S5LV0614P0_20000619_HOL_82)

83 A survey of suitable methods is outside the scope of this paper but might include a hardware trusted computing base, cryptographically signed and verifiable audit trails of program code and data, and multiple simultaneous distributed log files

84 Aidan Wills, Mathias Vermeulen 2011: Parliamentary Oversight Of Security And Intelligence Agencies In The European Union (http://www.europarl.europa.eu/committees/en/libe/studiesdownload.html?languageDocument=EN&file=48800)

85 Commission nationale de contrôle des interceptions de sécurité - 18ème rapport d'activité - Année 2009 http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/104000489/0000.pdf

retrospectively. The Commission also ensures **prior** authorization of all interception warrants (turning round emergency requests within one hour), which are capped below a fixed number expressly for the purpose of protecting civil liberties. Authorizing departments must apportion this quota ceiling between themselves, and make provision for their own contingency reserve. Recently the independence of CNCIS was tested by a complicated political scandal about circumvention of procedures by the country's most senior intelligence official, whose objective was to trace the communications of journalists at *Le Monde* and inhibit their exposure of illegal donations to the governing party[86].

Case studies which don't stack up

This year the IoCC has endorsed[87] several "case-studies", six of which are offered in support of present policy on communications data (studies 2, 3, 12, 13, 14, 15). However from easily traced media reports, a different picture emerges which prompts some skepticism about the impression he gives

- Case Study 2 – it isn't clear if the suspects were identified from cellsite analysis (but that may be the case). It isn't clear if other investigative means might have identified the suspects. Once the suspects had been identified, it appears substantial other evidence was available and obtained.
    - "officers were led to Kinson Common on April 8 during a surveillance operation on target suspects... As the search continued so did the surveillance operation and Lammali was spotted with friend Ryan Dear collecting something in a holdall from an area of nearby Redhill Common. They were stopped by officers and found to be in possession of five further shotguns belonging to Mr Langdown."[88]
- Case Study 3 – concerns access to subscriber data to confirm the identity of an already known suspect, and thus does not demonstrate any necessity for prior retention of traffic/location data.
- Case Study 12 – the suspect was not identified using communications data. The case could not be traced, so it isn't clear whether another investigative strategy could have led to a successful prosecution
    - A fingerprint from the scene identified a suspect from the Northampton area and two of his known associates subsequently became suspects. Mobile telephones were identified for the three suspects
- Case Study 13 – the suspect was not identified using communications data. News reports indicate that blanket retention was not necessary for detection or prosecution
    - "Police investigating the assault and robbery in Kilmaurs found traces of his DNA on a handbag and arrested Gable as he arrived back from a trip to Northern Ireland on a ferry. Specialist software was used to download information from the sat-nav device in his car. It located him at or close to each of the crime scenes. He was found to have been just 20 seconds away from one of the auto tellers he used to steal cash"[89]

86 http://fr.wikipedia.org/wiki/Affaire_Bettencourt#Violations_pr.C3.A9sum.C3.A9es_du_secret_de_l.27enqu.C3.AAte_et_du_secret_des_sources

87 IoCC Annual Report 2011 ibid.

88 http://www.bournemouthecho.co.uk/news/districts/bournemouth/9341126.How_violent_Bloxworth_robbers_were_caught/?ref=rss

89 http://www.bbc.co.uk/news/uk-scotland-glasgow-west-15491273

- Case Study 14 – concerns access to subscriber data to confirm the identity of an already known suspect, and does not demonstrate any necessity for prior blanket retention of traffic/location data.
- Case Study 15 - the identity of the suspect was already known, and a strategy of communications data preservation may well have been sufficient for prosecution of ongoing offences.

Thus only one out of six relevant case studies gives plausible support for the strict necessity (rather than mere usefulness) of prior blanket retention of the entire population's traffic and location data. Allowing that news reports may not tell the whole story, nevertheless if the IoCC is retailing these cases at face-value, presumably chosen for their persuasiveness, what does this tell us generally about his standards of logical rigour in applying a test of necessity?

What does the IoCC consider "necessary and proportionate" ?

Under the UK regime, almost all jurisprudence about interception and communications data takes place invisibly within the cranium of the IoCC, and almost nowhere else.
On pp.27 of the 2011 report it states that inspectors

- "seek to ensure...the disclosure required was necessary and proportionate to the task in hand"

The IoCC was asked by the Open Rights Group (ORG) to explain the methodology for verifying that authorizations/notices scrutinized by random sampling were in fact necessary and proportionate. For example, is it the IoCC's view that his functions are discharged if he satisfies himself that the designated person believed at the time the authorization was necessary and proportionate, or does the IoCC apply his own judgment of necessity and proportionality, or does he use a test such as the "manifestly unreasonable" standard for judicial review? Here's the reply:

(21/8/12) The inspectors examine the justifications for necessity and proportionality that have been set out in the application. The inspectors will also scrutinise the decision made by the designated person (recorded in their written considerations). The necessity and proportionality tests for communications data are quite specific – in order to justify **necessity** under Section 22(2) the applicant **must make the link** between the crime/offence (or other purpose), the suspect, victim or witness; and the phone or communications address

– in order to justify proportionality the applicant must explain **how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation**, provide a justification as to how the specific **date/time periods requested are proportionate** and **consider, if relevant,** whether the objective could be achieved through less intrusive means. **Collateral** intrusion must also be considered and any **meaningful** collateral intrusion described (for example, the extent to which the privacy of any individual may be infringed and why that intrusion is justified in the circumstance). The case must be made for each specific data request and the application supporting the request should stand on its own. If the inspector has concerns that the tests have not been met, they will speak to the applicant and/or the designated person. The inspector may also ask to see further supporting documentation (such as the case file, policy logs, operational book etc).

These replies raise many questions about the spirit of ECHR compliance, without concrete information illustrating what is and is not judged acceptable. How many people's data can be accessed to investigate what types of crime, what happens to that data subsequently,

especially if something unexpected is found? Can a request be widened if nothing is found initially? Is anything done systematically to detect attempts at fishing expeditions? What is the policy on disclosure of communications data access to defence counsel? There is no published policy on any of these matters.

The IoCC was also asked about patterns of communications between people and websites (see above **Inferring "sensitive data" from the social graph**) and whether he applied particular safeguards, or required a higher level of justification, for this mode of analysis. He replied:

All communications data requests are protectively marked under the Government Protective Marking Scheme (GPMS). Once **disclosed**, the communications data is subject to DPA. DPA is not overseen by the Interception of Communications Commissioner.

This reply illustrates a key deficiency of the current oversight regime, which fails to regulate the *modalities of analysis* of information about private life which is in scope of ECHR Art.8, but may be wholly or partially exempted from Data Protection, and treated as out of scope by the IoCC. The nature and application of the algorithms used for data-mining and traffic-analysis may seriously infringe human rights; this is a serious lacuna in UK legislation.

August 2012

Appendices

Queries about police oral evidence given to Joint Committee

Both Gary Beautridge and Trevor Pearce (repeatedly) confused the Interception Commissioner with the Information Commissioner in their evidence, casting some doubt about their actual familiarity with oversight procedures.

However there is a much graver concern about the good faith of the police evidence to the Committee on 12th July[90], when it was stated:

(Q142) Peter Davies: For some time it has been possible, roughly or more precisely, to locate a mobile telephone through the use of communications data. A team I have led has used that as almost the **sole** means of detecting a serious double murder in one of my previous forces ....(Q146) ...related to a retired couple shot dead in their home on the coast of Lincolnshire in August 2004 by, as it turned out, the pre- eminent organised crime group then operating in Nottinghamshire. Bluntly, without communications data relating to contacts between mobile phones **it would not have been possible to detect that crime** and lock up the people responsible. ..(Q147)...Bluntly, there were other people involved in the conspiracy whom it might have been possible to prosecute and convict, but who it but who it was not possible to prosecute and convict **because there was a data loss** in that investigation

Tracing this case using the details provided leads to news reports suggesting this account is materially misleading :

> **Police failed to protect innocent couple executed in gangland revenge attack, damning watchdog report reveals**[91]
>
> The IPCC upheld five of seven complaints made by the Stirlands' family. They found:
>
> - After the shooting incident at their Nottingham home, Mr and Mrs Stirland were given neither protection nor help by Nottingham police.
> - That incident was "not properly investigated, despite rumours circulating about who was responsible".
> - Nottinghamshire Police's failure to share intelligence with Lincolnshire Police about the threat to the Stirlands was "unacceptable".
> - The response to Mrs Stirland's call about the prowler was "delayed and unsatisfactory".

Moreover it emerged two years later at the inquest that

> **Stirland revenge hit men 'known before killings'**[92] Police had identified Nottingham crime boss Colin Gunn's **team of six hit men weeks before** two killed a couple in a revenge attack, an inquest jury heard....The former officer, who remained anonymous, said the two men who killed the Stirlands had been named as part of Gunn's team of hit men.

Although this case was offered in evidence as an illustration of the necessity of blanket data retention, in actuality it precisely illustrates how diligent and proactive use of targeted data preservation could both prevent and detect crime. Had communications data *preservation* commenced promptly about suspects identified weeks before the crime, *prima facie* police might well have been able to prevent the crime as well as catch the perpetrators.

---

90 http://www.parliament.uk/documents/joint-committees/communications-data/uc120712Ev3HC479iii.pdf

91 Daily Mail 22nd February 2008 (http://www.dailymail.co.uk/news/article-517442/Police-failed-protect-innocent-couple-executed-gangland-revenge-attack-damning-watchdog-report-reveals.html

92 BBC News Online 3rd Feb 2010 (http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/8496826.stm

Furthermore, it emerged, contrary to the conclusions of the IPCC investigation[93] that:

> **Corrupt officer fed data to Colin Gunn on Stirlands[94]** A corrupt detective searched Nottinghamshire Police computers for intelligence about a couple killed in a gangland execution, an inquest heard.

It seems ironic that the police cite a fatal case of police corruption and its subsequently botched investigation, as justification for blanket retention of data about the entire population. It would be more logical to propose blanket retention of data on the entire police force. This is probably not the conclusion drawn by the Committee from the evidence heard.

Costs estimates for prior judicial authorization to access traffic data

In the 7th July evidence session[95], Angela Patrick of JUSTICE made the suggestion (Q274) that additional costs for introducing prior judicial (magistrate) authorization to access data could be estimated by extrapolating corresponding Home Office figures provided for the Protection of Freedoms Act (which required local authorities to get magistrate approval)

Here is the calculation, based on the Home Office's published estimates for PoFA[96] (£ 670k p.a), and the new 2011 Interception Commissioner's report.

Local authorities requests comprise 0.4% of the total (pp.39 IC). Suppose magistrates ought to approve the 48% (pp.29 IC) of requests comprising traffic or usage or location (or combined) data - i.e. all requests not purely for account subscriber data (pp.29 IC). The rationale is that subscriber account data is retained anyway, and that does not reveal dynamic behavioral data which is very privacy sensitive.

Therefore the initial estimate = 0.670 / (0.004 x 0.48) = £349m per year
However, there is a discrepancy, because the the Home Office figures say "we have assumed there will be **5,500** authorizations based on last year's usage (and we assess the magistrate's assessment will take 20 mins)", whereas the IoCC says "during the period covered by this report 141 local authorities notified me they had made use of their powers to acquire communications data, and between them they made a total of **2,130** requests. This is an increase from the previous year's figures (134 local authorities, 1,809 requests)."

Accordingly we reduce the £349m figure pro rata: (2130/5500) * 349 = **£135m per year[97]**
It should be emphasized this estimate is an upper bound based on a large extrapolation. A comprehensive system which integrated prior judicial authorization of interception warrants and communications data, could triage different cases to specialized magistrates, and so be much more cost effective overall[98].

---

93 http://www.ipcc.gov.uk/documents/stirland.pdf

94 BBC News Online 17th Feb 2010 (http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/8496826.stm)

95 http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

96 RIPA and Local Authorities, IA No: HO0031 Final, Home Office 22/12/2010 http://www.homeoffice.gov.uk/publications/about-us/legislation/freedom-bill/ripa-local-ia?view=Binary

97 However, it might fairly be said that the magistrates considering traffic/usage/combined data requests will be making more complex decisions about proportionality and necessity. The Home Office estimates the total cost of magistrate's time as £365/hr (inclusive of court overheads)

98 The French CNCIS regime is not based on separate judicial authorization, but manages prior scrutiny of both interceptions and communications data access, with organizational independence, at much less cost

BT

BT welcomes the Government's review of Communications Data and Interception Powers and we are pleased to have the opportunity to submit our views on such an important subject.

When we met recently to discuss the review, you made clear your understanding that it was the Government's intention for a "lawful interception" regime to continue. I can confirm at the outset that BT is supportive of this, subject to any new regime being proportionate and having due regard to human rights. BT's Chief Executive, Gavin Patterson, expressed the view at the World Economic Forum meeting in Davos in January 2014 that the right to privacy is not absolute and must be balanced against the requirement for national security.

The Internet Service Providers' Association response to this review asserts that law enforcement authorities should have "reasonable lawful access" to communications data (and, by implication, communications content) in order to help in the detection and investigation of serious crime and to safeguard national security.

As I have said, we at BT endorse this view. We consider that it is appropriate to maintain a regime that permits access to content and communications data, provided that the circumstances are suitably circumscribed, and provided that all necessary checks and balances are in place to ensure the lawful and proportionate operation of that regime, particularly from a human rights perspective.

Your current review is very timely- and indeed essential, given the significant technological and legal developments since the Regulation of Investigatory Powers Act 2000 (RIPA) was enacted, not least the EU Court of Justice (CJEU) judgment on the Data Retention Directive, and ongoing pressure for greater transparency. Annex 1 answers the questions in your letter. Annex 2 reflects our views on certain aspects of RIPA and other statutory provisions. I have also set out below the broad principles that BT considers must be reflected in a revised regime:

(1) All requests made of Communications Service providers (CSPs) and other service providers must be lawful and take account of international human rights principles, especially those under the European Convention on Human Rights

This may be a statement of the obvious, but you will be aware, especially since the Snowden revelations, of the different contexts in which the legality of alleged mass surveillance and data retention have been challenged from a human rights perspective . We have a number of substantive observations in this context in relation to section 8(4) RIPA. DRIPA and section 94 Telecommunications Act 1984 (see Annex 2). You will note in particular that we believe that it is imperative for Government to introduce proposals for a successor to DRIPA well in advance of the sunset clause and that they should contain greater privacy protective measures.

In reality, case law is consistently evolving. It is not clear how the mass surveillance or (putative) data retention challenges will conclude, and new legislation may well be introduced in the UK before these issues are resolved. We believe, however, that a number of procedural steps could be introduced to strengthen the regimes going forward, and to address public and privacy stakeholder concerns (see below).

The human rights agenda for business has also attracted growing attention from governments, NGOs, investors and the media for some time. Some of this interest has undoubtedly been triggered by the post-Snowden debate on surveillance and interception, the subsequent legal challenges that have been brought, by Privacy International and others, and by the recent CJEU judgment invalidating the Data Retention Directive. You will also be aware that UK listed companies face increasing obligations to report on their position on human rights.

In the present context, communications companies (and other relevant service providers) will be expected to take steps to satisfy themselves, to the extent practicable, that whatever they are asked, or compelled, to do by government is prima-facie human rights-compliant, especially regarding the right to respect for private and family life. In addition, companies face pressure to be more transparent, where possible, about the activities they undertake in this area.

Our view is that the fundamental principles of a revised regime (the *"what')* must be Article 8 compliant (see Annex 2). In the light of the comments above, we would also ask you to consider the following suggestions on process (the *"how") :*

- Formal requirement for CSPs/ service providers to be consulted about certain warrants/ notices (e.g. section 8(4), DRIPA);

- Judicial/Investigatory Powers Tribunal (IPT) oversight/ approval for the issuing those warrants/ notices, and in particular, since they are not tied to specific individuals or premises, for "external" warrants (i.e. those granted in respect of communications sent or received outside the British Islands). Consideration could be given, for example, to requiring prior approval from the IPT for external warrants, on production of details on the need for the warrant and the measures taken to avoid any privacy intrusion; a special advocate could be appointed to consult with human rights groups to the extent possible and to contest the grant of that warrant.

- Formal mechanism for CSPs/ service providers to seek speedy review of those warrants/ notices. Currently, the only route available to challenge a DRIPA notice is via judicial review;

- Review of the requirement for secrecy. We understand the requirements for secrecy in particular contexts, but believe that government should consider providing more information where possible, for example about the number and nature of DRIPA notices served. Where government considers that additional transparency is not possible then it should explain why not;

- Greater oversight in relation *to* the interception of external communications (for example, the appointment of a special representative with a human rights background and express mandate to assist the Interception of Communications Commissioner (IoCC). The IoCC could also be given the power to refer a particular issue to the IPT if he is concerned about the use of surveillance powers; and

- Encourage the IoCC to continue to provide as much information as possible in his annual report and suggest that he should be under a duty to report on the filtering operations conducted on the product of external interception to provide more transparency and openness about this aspect of the surveillance regime.

(2) <u>The regime must reflect technological developments since RIPA was introduced</u>

Your letter asked questions about changes in technology. Our detailed answers are at Annex 1, but you may also find it helpful to have a brief summary. In short, we think that RIPA is a more logical starting point for technological analysis than the Communications Data Bill of 2012, despite the fact that it has not stood the test of time.

RIPA is essentially rooted in the traditional PSTN telephony model, in which content can be readily distinguished from traffic data, and fixed point interception is relatively straightforward. The reality now is that the development of internet services has changed the landscape, which continues to evolve. In particular, the rapid growth of cloud-based services, with data hosted outside the UK by companies outside the UK, means that very significant amounts are retained by bodies other than CSPs. The

telecommunications industry is moving away from traditional fixed-line service to cloud-based architecture (Network Function Virtualisation), which will itself require a cloud-based interception capability for law enforcement purposes. So, new models, from both a technological and a financial perspective, will be required for retention and interception.

The extent to which these and other developments will impact on the framework and/or key provisions of a revised statutory regime is no doubt something for you to consider in the course of the review. But it is worth flagging some specific examples which impact on key concepts in RIPA. Firstly, the notion that the most efficient means of intercepting external communications is at the physical edges of the jurisdiction is no longer valid. This may have implications for the distinction between internal and external communications for interception purposes. Secondly, whilst the distinction between content and traffic data remains clear-cut for telephony, it is far less so for online communications and increasingly obscure from a cloud services/social media perspective, where communications data is often embedded in content. The traditional content/ traffic data distinction has a key role under RIPA, but is not entirely fit for purpose going forward.

.

(3) The regime must apply a level playing field for all service providers

In our view, in principle, all providers of communications services in the UK should be treated equally under lawful intercept/ retention regimes. This ensures competitive fairness and reduces the risk that users move to alternative means of communication to avoid scrutiny. Whilst there may be enforcement issues for providers based outside the UK who do not have significant infrastructure in the UK, we do not consider that the larger UK CSPs, such as BT, should be required to step in to provide assistance unless all reasonable efforts have been made by government to secure assistance from the relevant service provider, who will have control over the service. The correct guiding principle is that the service provider best placed to comply with a request should be asked first, irrespective of their size or location.

(4) Cost recovery must be provided for in the regime

It is not right that government should have discretion as to whether to reimburse service providers for the costs they incur in complying with the regime. All eligible costs should be met by government, to ensure that our shareholders are not being asked to fund those aspects of national security that should properly be met by government.

Finally, and on a separate note, I would like to flag our concerns regarding RIPA section 3(3). These are addressed in detail in Annex 2, but the fundamental issue is worth reiterating here. We have long been concerned that in filtering content on a voluntary basis, which Government continually exhorts us to do, the CSPs run a legal risk under RIPA. We have made this point repeatedly to Government and believe that it is imperative for them to resolve this issue if the dialogue on the filtering of unsuitable content is to move forward.

I trust that the views BT has expressed in this letter and its Annexes are helpful. My colleagues and I would welcome the opportunity to discuss matters further with you and David Anderson QC. You will note in particular from Annex 2 that there is some additional information that we would like to make available to you.

Mark Hughes
President BT Security

Annex 1

Here are BT's replies to your questions :

Q: What are the changes and developments in communications technology, services or methods that need to be taken into account by the government in framing legislation on interference 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.

- We believe that the Regulation of Investigatory Powers Act 2000 (RIPA) is a far more appropriate starting point for this review than the draft Communications Data legislation from 2012. The technological leaps in recent years have driven a shift from analogue to digital and IP based services. Interception law is based on concepts from the 1970s and telephony/dial up services. It has not kept pace with the development of IP-based communication services and the vast amounts of data that they can transmit;
- For example, RIPA distinguishes between those communications which are sent and received in the UK ("internal") and those which exit or enter the UK from overseas ("external") and treats the two quite differently for interception purposes. However, the concept of the 'edge of the territory', which underpins this distinction is no longer an appropriate point of divide, given how IP networks work . Communications sent by UK residents for UK residents do not transit purely within the UK, but could travel around the world on their way from sender to recipient, and data which relates to 'internal' communications can be held on servers internationally and not just in the UK. In addition, routers serving external traffic either entering or exiting the UK may be situated anywhere within the UK not just at a point which would be considered 'edge of the territory' ;
- The rapid growth of cloud based storage and service applications, for example semi-anonymous social media services, impacts on both the ability of CSPs to retain data, and on the ability of law enforcement agencies (LEAs) to obtain data. Many cloud services are offered by companies which are based outside the UK, and which host their data outside the UK (for example Google, Facebook and Microsoft) . The increasing use of end to end encryption in such technologies further reduces the effectiveness of traditional interception methods:
- The huge volumes of data generated by IP services and the decreasing lifespan of new applications and services mean that the most practical way of obtaining information might be to extract it after the event on a targeted basis, rather than by means of real-time interception. Another major development is that many communication companies are moving from traditional fixed line service provision to a cloud based architecture approach called Network Function Virtualisation (NFV). In NFV, traditional hardware network infrastructure, such as a PSTN local exchange, is replaced by a virtual entity running in a virtual data centre, which could sit anywhere in the world. This development would make 1970s style fixed point interception unworkable- the technology used for lawful interception would itself need to become a cloud provided service. Such technological

developments present Communications Service Providers (CSPs) with considerable challenges in achieving and maintaining the security of legal interception arrangements and related critical national infrastructure considerations; and

- We are also seeing a significant increase in the speed with which new services are both brought to the market and withdrawn (e.g. apps provided by Apps stores). For example, new apps can now be added to App Stores and quickly gain significant volumes of users. So, arrangements with government under which CSPs notify, design and install any agreed interception capability must be able to keep pace with these developments, and government must in turn let CSPs know their requirements more quickly.

Q: 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 there continues to be a difference between communications data generated, processed and in some cases retained by a CSP for either charging or operating the underlying communications service, and the content of those communications. The growing volume of that communications content results in the continuing need to treat these two separately. (On the other hand, in the case of cloud services and social media communications, the distinction between the two is not at all clear, as "communications data" is often embedded in communications content.);
- The Communications Data Bill continued the distinction between traffic data and content which originated from RIPA We consider that this remains a valid approach for telephony, where the distinction is clear cut, but that it is problematic when considering the potential intrusiveness of an interception of a communication on the internet. Disclosure of traffic data does not currently amount to an interception under RIPA, but the question as to what is and what is not traffic data remains unclear;
- There is no helpful case law and at present, the Home Office RIPA Guidance provides that, for example, filtering at domain level is not an interception for RIPA purposes because only traffic data is disclosed. However, filtering at (say) page level does amount to an interception, because information beyond the first "/" amounts to content. This view is repeated in the latest draft Code of Practice on the Acquisition and Disclosure of Communications Data published by the Home Office;
- This distinction is not an arbitrary one, but one that nevertheless has conceptual difficulties, since disclosure of domain name alone in some cases can be potentially very intrusive; and
- It is clear in any event that the distinction between communications data and content needs to be reviewed. There should be a system of oversight that ensures that the interference arising from any interception is proportionate.

Q: Is the subdivision of communications .data into subscriber, user 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?

- These definitions have never been properly enunciated and so we do not think that they adequately reflect the relative intrusion into an individual's privacy. As indicated earlier, we do not think that the content communications data distinction is entirely fit for purpose either- and this whole area needs to be reviewed, taking due account of the relevant parts of the CJEU judgment on the Data Retention Directive and the approach taken in the E Privacy Directive, where the emphasis is on an individual's right to privacy.

Q: How should the government address the challenges to lawful interference with communications that arise from communications services being provided to people in the UK from foreign countries?

- We agree that government should be able to enforce obligations on any globally based service provider that provides services to users in the UK. We also think that the review should consider the legal position where services are provided in one country but the related communications data is processed, generated or stored in another country; and
- In principle there should be parity of treatment for overseas providers with limited (or no) UK infrastructure and UK based companies with large onshore infrastructures. Services to UK users should only be provided if the service provider enables appropriate retention and interception capabilities to meet LEA requirements. This should apply to all sizes of service provider on a level playing field.

Q: 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 co-operate with the British Government?

- We are concerned that large CSPs such as BT should not be treated as a first 'port of call' for requests in this context and would seek to obtain express assurances in any new legislation that this will not be the case. Whilst we acknowledge the practical difficulties in ensuring compliance of overseas CSPs, government should only look to UK based CSPs for assistance as a last resort; and
- One option might be to include an obligation to provide adequate retention and interception capability in the General Conditions made under the Communications Act 2003 . This would mean that Mutual Legal Assistance Treaty ('MLAT') arrangements could be used.in the event of non-compliance by overseas service providers. Existing MLATs may need to be updated to take account of revised arrangements and in the

longer term more specific EU or wider international arrangements may be required.

Q: Should the government seek a single international regime for the operation of lawful interference with communications? If so, what might be its principal features?

- Any international regime would need to be one built upon respect for human rights and due process, where interception of communications is thought to be necessary. Different countries view these things differently and we question the practicality of creating an international regime in these circumstances.

Q: 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 material from you and other providers?

Taking each of these in turn:-

- **Single Point of Contact** ('SPOC') arrangements have generally worked very well. We support their continued role in the revised arrangements for interception and data disclosure.
- **Request filters**. In principle we do not think that it is appropriate for companies that provide communications services to be involved in editing their customer's private communications before these are sent to law enforcement agencies. Whereas government may make a case for getting hold of data and compelling its surrender, it is quite a different matter to then require service providers to inspect and edit that private data before it is handed over.
- We also have the following concerns about the suggestion that CSPs should operate any filtering of communications data prior to that data being made available to the relevant agencies:
  - i) CSPs are currently required to provide an exact copy of the information they hold which has been requested by an agency. CSPs are not competent to interpret or filter that information. CSPs have no knowledge of the background to individual requests. Those parties who have requested the information are best placed to undertake any filtering;
  - ii) Filtering out information results in an imperfect copy of the original. This could damage the evidential integrity and value of the information delivered (and so impact on the admissibility of the evidence);
  - iii) Filtering may not be 100% predictable in all cases with regard to inclusion and exclusion of records; and
  - iv) CSPs should not be responsible for having to take decisions - automated or otherwise - for any over or under-delivery of information as a result of filtering before delivery of information to the requester. Any legislation

purporting to introduce a requirement of prior filtering would need to exempt CSPs from any potential liability as described above, and clearly place the onus on the party requesting filtering to ensure the sufficiency and adequacy of the information provided to them.

- Deep packet inspection -'DPI' - We do not see how the precise extraction of a limited set of data can be achieved simply from a high bandwidth connection with some form of DPI capability. Whereas DPI kit generally is very capable, the challenge would be to deploy the DPI kit in the best place in the network to gain sensible access to the communications travelling on it , and then to configure it so that it correctly extracts only the required information;
- Additionally, deployment of DPI kit on a large scale creates significant physical issues in terms of housing the kit, providing power and cooling facilities, and connectivity in locations which currently may only have existing limited resources. There is also the risk that this equipment may cause a failure in the network to which it is connected. This could clearly have serious consequences for the CSP concerned, including loss of services to customers and potential financial liability under customer contracts and customer service guarantee schemes;
- The risks described earlier in relation to data integrity issues arising from filtering would also be relevant if DPI capability were used. Furthermore, with the increase in signalling encryption, and privacy by design (use of temporary identifiers between network elements to prevent tracking or 'man in the middle' attacks}, DPI interception of communications data or content is likely to become a less practical option (notwithstanding the data rate challenges);
- We therefore would consider on-switch *I* on-database approaches to be the best option in the first instance with the use of DPI only as a last resort; and
- The speed and accuracy with which intercept capability can be deployed is of course extremely important to government and a system which facilitated electronic requests would clearly be advantageous to government. However, we would not support a facility that afforded government direct access to CSP's infrastructure to set up lawful interceptions. CSPs must ultimately be able to control what interventions are made, to ensure that content of communications is not inadvertently disclosed and customers' privacy compromised.

Q: 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?

- In principle, we have doubts about CSPs being involved in decrypting communications - that is a matter for government.

Q: What more could be done to exploit the communications data and intercept that is currently available and likely to continue to be so?

- Over the top service providers such as Skype could be required to provide the same level of lawful interception support to law enforcement agencies as is currently required from CSPs with infrastructure ; and
- Those public authorities requesting communications data should be able to make better use of certain communications data that is already available to them, but which we consider to be underused (eg information contained in Wi-Fi access logs).

Q: 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?

- We submit that government should pay all CSPs' eligible costs without exercising any discretion as to whether to pay or not;
- Under the current data retention arrangements, many CSPs simply 'top up' their existing business records with additional retained data for the required retention period when otherwise they would not have retained that data for their business needs. A data preservation model would probably require all communications data relating to a particular target to be identified and stored separately and securely away from CSP's own business records, thus duplicating the data retained, and potentially substantially increasing the amount of storage required, and the people needed to manage such a solution; and
- Leaving aside costs. a data preservation model may pose compliance challenges that the current model does not (e.g. ensuring that the system does not over or under-select data for retention.

How should the government organise its relationship with communication service providers, both when framing legislation on interference with communications, and routinely?

- We would like to see effective consultation and a more constructive dialogue between government and CSPs at any early stage of proposals, so that CSPs' views can properly be taken into account before any final decisions about policy or legal changes are actually made;
- We would also like a more strategic engagement with government so that CSPs can contribute more effectively, as the current arrangements for dialogue are fragmented and inconsistent. This has been particularly illustrated by our attempts to engage with Government about our concerns over the treatment of content filtering under RIPA; and

- Operational engagement with the SPOCs works well and we would like to see this arrangement maintained in its current form.

Q: 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.

Please see confidential material included in Annex 2.

***

October 2014

The Center for Democracy & Technology

1. The Center for Democracy & Technology ('CDT') is pleased to submit this written evidence as of the Investigatory Powers Review concerning Part 1 of the Regulation of Investigatory Powers Act ('RIPA') 2000, as amended by the Data Retention and Investigatory Powers ('DRIP') Act 2014.

2. CDT is a non-governmental organisation that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communications technologies. Since its founding 20 years ago, CDT has played a leading role in shaping policies, practices and norms that empower individuals to use these technologies effectively as speakers, entrepreneurs and active citizens. Whilst based in Washington, DC, CDT also has a presence in London and Brussels.

Introduction and Recommendations

3. Our evidence addresses three major aspects of RIPA (as amended) that, in our view, fail to comply with customary international law or the European Convention on Human Rights ('ECHR'). We have also highlighted some relevant aspects of US law governing surveillance in criminal cases for comparative or illustrative purposes.

4. Part I of our evidence assesses Section 4 of the DRIP Act, which empowers the Secretary of State for the Home Department to issue interception warrants that are intended to have extraterritorial effects; we conclude that such warrants, if issued, would violate customary international laws pertaining to state sovereignty and would also—at least in the United States—compel telecommunications service providers to violate local law. Parts II and III then address two features of the RIPA/DRIP regime that are incompatible with Article 8 of the ECHR: the authorities' power to engage in potentially unlimited collection and storage of communications data under Chapter II of RIPA, and the Secretary of State's virtually unfettered power to issue retention notices under Section 1 of the DRIP Act. In the context of retention notices, we describe the US system of data preservation orders, which we believe adhere more closely to human-rights principles.

5. **We respectfully suggest that your recommendations should include the following:**

   - **Parliament should immediately repeal the extraterritorial provisions of Part I of RIPA (as amended by Section 4 of the DRIP Act), on the basis that they violate the UK's binding obligations under customary international law.**

- **In the interim, the Secretary of State should refrain from issuing any extraterritorial interception warrants in order to avoid a violation of binding customary obligations (and avoid compelling telecommunications service providers to violate other States' domestic laws).**

- **Parliament should mandate that when the Secretary of State believes the interception of communications outside of the UK's territorial jurisdiction is necessary and proportionate in the context of UK investigations or proceedings, she must adhere to the processes set out in mutual legal assistance agreements or other international agreements, or otherwise pursue disclosures through formal diplomatic channels.**

- **If the Secretary of State retains the ability to issue extraterritorial interception warrants, primary or secondary legislation should provide that such warrants cannot compel disclosures that are not permitted by local law.**

- **Parliament should adopt legislation requiring that authorisations or notices for obtaining or disclosing communications data (including under Section 8(4) warrants) be restricted to data concerning a single person or set of premises.**

- **The legislation should also restrict the grounds on which the authorities may access communications data to those grounds that are strictly necessary for safeguarding the UK's democratic institutions (to include the protection of public safety and the prevention of serious crime).**

- **Parliament should repeal Section 1 of the DRIP Act and replace the Secretary of State's power to issue data retention orders with a power for law-enforcement officials to issue data *preservation* orders that relate to individual users' data, where that data is required for specific investigations or proceedings.**

- **If the Secretary of State retains the ability to issue data retention orders, Parliament should amend RIPA and the DRIP Act to provide that these orders are only valid with respect to data stored within the territorial jurisdiction of the UK, that the orders may only require the retention of the communications data of a specific individual named in the order and that they cannot be issued unless the retention is necessary and proportionate with respect to the individual in question.**

6. Like RIPA, this submission uses the term 'communications data' to refer to data describing communication, such as its sender, recipient, date, time, location and duration. The term 'interception' refers to the collection of the content of a communication.

I. Section 4 of the DRIP Act violates binding customary international law norms and would compel US telecommunications service providers to violate US law

7. In our view, insofar as Section 4 of the DRIP Act purports to empower the Secretary of State to issue interception warrants that would impose an obligation upon persons outside of UK territory, the legislation violates customary international law and should be repealed.

8. Customary international law is binding upon the UK[1], and one of the best-established rules found in that body of law is that in the absence of a permissive international-law norm to the contrary, a State '*may not exercise its power in any form in the territory of another State.*'[2] As a corollary of this rule, '*[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.*'[3]

9. Thus, any attempt by the UK to enforce an interception warrant in another State's territory would violate the binding customary rule of territorial sovereignty and constitute a serious breach of the international order.

10. One reason this customary norm is of critical importance is that a warrant or order compelling action in another State could force an individual or company to violate the domestic law of that State. Such a development could have serious implications for international relations and raises concerns about a lack of due regard for the international- law principle of comity.[4]

---

[1] *See Jones, R. v* [2006] UKHL 16 (29 March 2006), ¶ 11 (Lord Bingham).

[2] *S.S. 'Lotus'*, Permanent Court of International Justice, Judgment, Series A, No 10 (7 September 1927), p. 18; *see also Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, International Court of Justice, Judgment (Merits) (27 June 1986), ¶ 205 (finding that the customary principle of territorial and political integrity '*forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States*').

[3] Restatement (Third) of Foreign Relations, § 432(2), including comments (b)-(c) and list of sources.

[4] *See generally Viking Line ABP v International Transport Workers' Federation & Anor* [2005] EWHC 1222 (Comm) (16 June 2005). We understand the principle of comity to include not only concerns related to the jurisdiction to adjudicate, but also to the jurisdiction to prescribe (or issue judicial or administrative orders): *see Hilton v Guyot*, 159 U.S. 113, 163-164 (1895) (describing comity as '*the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons was are under the protection of its laws*'). *See also Hartford Fire Ins Co v California*, 509 U.S. 764 (1993) (discussing, in relation to comity, the relevance of the existence of a conflict between US and UK law).

11. For example, in the United States, the Electronic Communications Privacy Act ('ECPA') prohibits communications service providers from disclosing the content of an electronic communication within the first 180 days of the provider's storage of the communication, except pursuant to a warrant issued by a US judge or magistrate; this requirement applies regardless of the nationality of the communication's sender or recipient.[5] Moreover, a US federal appellate court (the Sixth Circuit Court of Appeals, whose rulings are binding within several US states and serve as persuasive authority in the other federal judicial jurisdictions) has found that under the Fourth Amendment to the US Constitution, a warrant is required even for content that is over 180 days old.[6]

12. In other words, at least within the Sixth Circuit, communications service providers cannot legally disclose communications content in the absence of a warrant issued by a US judge or magistrate based on a finding of probable cause. In our experience, providers in the US generally follow this Sixth Circuit ruling on a nationwide basis.

13. The DRIP Act, however, purports to require communications service providers in the US to disclose communications content without having first been served with a US judicial warrant based on a finding of probable cause. This requirement contradicts both ECPA and the US Constitution.

14. We are aware that as amended by the DRIP Act, RIPA seeks to impose an extraterritorial duty to give effect to a UK interception warrant only when it is '*reasonably practicable*' for the recipient to take the steps necessary to give the warrant such effect. In determining whether the steps a foreign entity must take are 'reasonably practicable', the DRIP Act provides that '*regard is to be had*' to the requirements of local law and the extent to which the interception warrant may be given effect without breaching that law.

15. We view this non-binding consideration as wholly inadequate to preserve the sovereignty interest that States have in controlling the execution of searches within their borders.

16. For all of the foregoing reasons, we respectfully recommend that Parliament repeal the extraterritorial provisions of Part I of RIPA as amended by Section 4 of the DRIP Act. If Parliament declines to do so, we respectfully recommend the adoption of either primary or secondary legislation providing that extraterritorial interception warrants cannot compel disclosures that are not permitted by local law.

17. For the same reasons, we recommend that Parliament require the Secretary of State to adhere to the processes set out in mutual legal assistance agreements or other relevant international agreements, or otherwise pursue formal diplomatic channels, when she believes that the interception of communications outside of the UK's territorial jurisdiction is necessary and proportionate in the context of investigations or proceedings within the UK.

---

[5] 18 U.S.C. § 2703(a).

[6] *US v Warshak*, 631 F.3d 266 (2010). The Fourth Amendment to the US Constitution establishes '*[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*'.

II. The authorities' exceedingly broad discretion to obtain communications data violates Article 8 of the ECHR

18. In our view, both the power to access communications data under Chapter II of Part I of RIPA and the virtually unfettered power to collect and use communications data obtained by way of interception warrants pursuant to section 5(6)(b) of RIPA are incompatible with the requirements of Article 8 of the ECHR.

19. As a general matter, the term 'communications data' includes 'the "who", "when" and "where" of a communication', whilst excluding the content of the correspondence.[7] It includes traffic data, service use and subscriber data.

20. We note that both individually and in the aggregate, communications data can reveal any number of intimate aspects of an individual's life, ranging from personal relationships to religious beliefs; sexual orientation; social, professional, educational and recreational activities; consultations with medical and legal professionals; reading habits; political activity; travel; and so on. As the Court of Justice of the EU ('CJEU') has observed in its judgment in *Digital Rights Ireland*, these data are particularly revealing when taken together and '*may allow very precise conclusions to be drawn concerning … private lives*'.[8] In some cases, the aggregation of such data may provide as complete a profile of an individual as the content of the communications would have done.

a. Article 8's requirements concerning communications data

21. Article 8 of the ECHR (taken together with Article 1) establishes that everyone within the UK's jurisdiction has the right to respect for his or her private life and correspondence, and that the UK public authorities are barred from interfering with this right except where such interference is both '*in accordance with the law*' and '*necessary in a democratic society*' in order to achieve certain legitimate aims.

22. As an initial matter, we recall the finding of the European Court of Human Rights ('ECtHR') that any public authority's collection of e-mail or telephone correspondence, or personal information pertaining to Internet usage, constitutes an interference with the right to respect for private life under Article 8.[9]

23. We further recall the Court's conclusion in *Malone v the United Kingdom* that an authority's collection of telephone communications data without the consent of the telephone subscriber also constitutes an interference under Article 8, as this data is an '*integral element*' of the correspondence.[10]

[7] 'Related communications data' for the purposes of Chapter I of Part 1 is defined under Section 20, while 'communications data' for the purposes of Chapter II is set out in Section 21(4)-(6). *See also* Home Office, Acquisition and Disclosure of Communications Data Code of Practice, ¶ 2.13 (hereinafter 'Code of Practice').

[8] *Digital Rights Ireland* (Judgment) [2014] EUECJ C-293/12 (8 April 2014), ¶ 27.

[9] *Copland v the United Kingdom* (2007), ¶¶ 43-44; *Liberty and others v the United Kingdom* (2008), ¶ 56.

[10] *Malone v the United Kingdom* (Plenary, 1984), ¶ 84; *see also PG and JH v the United Kingdom* (2001), 42; *Copland*, *supra* n. 9, ¶ 43.

24. It is clear, moreover, that the Court's finding concerning telephone communications data necessarily extends to data relating to such electronic communications as e-mail and general Internet usage. In other words, the requirements of Article 8 apply to the collection of electronic communications data just as they do to the interception of the content of correspondence. The recent CJEU judgment in *Digital Rights Ireland*, which found that the retention of communications data '*directly and specifically affects private life*' for the purposes of the Charter of Fundamental Rights of the EU, supports this view.[11]

25. The ECtHR's case-law has firmly established that in order for the UK to conduct secret communications-surveillance measures '*in accordance with the law*' for the purposes of Article 8, the public authorities must undertake those measures on the basis of a binding and publicly-accessible statutory law.[12] That law '*must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data*'.[13]

26. Moreover, the statutory law must set out, *inter alia*, '*the grounds required for ordering*' secret-surveillance measures.[14] Although the issuance of a surveillance order may involve some exercise of discretion on the part of the authorities, this discretion cannot be unfettered: '*the law must indicate the scope of any such discretion … and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*'.[15] Thus, a law that '*defines precisely, and thereby limits, the purposes*' for which the authorities are permitted to undertake the surveillance may meet Article 8's requirements.[16] By contrast, a law that does not clearly restrict and explain the scope of the executive's discretion, and particularly one whose list of possible grounds for surveillance is not exclusive, will not be compatible with Article 8.[17]

b. Application of Article 8's requirements to communications data under Part 1 of RIPA

27. We note that a warrant for the interception of '*external communications*' under Section 8(4) of RIPA, unlike an interception warrant under Section 8(1), does not contain any requirement that the warrant be targeted at a particular person or premises. We note further that a

---

[11] *Digital Rights Ireland*, *supra* n. 8, ¶¶ 26-29.

[12] *E.g.*, *Malone*, *supra* n. 10, ¶ 87; *Shimovolos v Russia* (2011), ¶ 68; *Weber and Saravia v Germany* (Decision, 2006), ¶ 95; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (2007), ¶ 76.

[13] *Shimovolos*, *supra* n. 12, ¶ 68; *Liberty and others*, *supra* n. 9, ¶ 62; *Weber and Saravia*, *supra* n. 12, ¶ 93.

[14] *E.g.*, *Shimovolos*, *supra* n. 12, ¶ 68; *Liberty and others*, *supra* n. 9, ¶ 62.

[15] *Malone*, *supra* n. 10, ¶ 68; *Liberty and others*, *supra* n. 9, ¶¶ 64-70.

[16] *Klass and others v Germany* (Plenary, 1978), ¶ 45.

[17] *See Malone*, *supra* n. 10, ¶¶ 71-80; *Liberty and others*, *supra* n. 9, ¶ 64.

warrant to intercept communications also authorises '*conduct for obtaining related communications data*' (section 5(6)(b)).

28. In respect of the power to access communications data under Chapter II of RIPA, we note that the purposes for which the designated UK authorities may obtain this data are both broad and numerous. Additionally, the designated authorities are not required to restrict their collection of communications data to items concerning any specific person or set of premises, or to destroy the data if its storage becomes disproportionate or unnecessary.

29. Section 22(2) of RIPA, as amended by Section 3 of the DRIP Act, allows the designated authorities to obtain and disclose communications data where such action is '*necessary*':

> *(a) in the interests of national security;*
> *(b) for the purpose of preventing or detecting crime or of preventing disorder;*
> *(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;*
> *(d) in the interests of public safety;*
> *(e) for the purpose of protecting public health;*
> *(f) for the purpose of collecting or assessing any tax, duty, levy [etc.] payable to a government department;*
> *(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating [such injury or damage]; or*
> *(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.*

30. The Secretary of State has previously made several additions to this list via the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006, and we observe that RIPA empowers her to make further additions in future.[18]

31. As with the power to intercept external communications under Section 8(4), Chapter II of RIPA does not require that an authorisation or notice for the collection of communications data be restricted to data concerning a specific person or set of premises. Instead, with only a few exceptions, Sections 22(1) and 23 of RIPA permit the designated authorities to collect '*any communications data*' from any current, historic or future time period, so long as the authorities believe the collection of that data is 'necessary' for any one of the purposes set out in Section 22(2) and is proportionate to the aim pursued.[19]

32. Thus, the power to obtain communications data from bulk interception under Section 8(4) warrants, taken together with the broad scope of access to communications data under Chapter II, grants the UK authorities an extremely wide scope of discretion to obtain and store any type or volume of communications data, pertaining to any individual or class of individuals (or, indeed, entire communities or nations), from any time period, for one of any

[18] Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006, SI 2006/1878.

[19] Code of Practice, *supra* n. 7, ¶ 3.5. There are some restraints on the type of communications data that the designated authorities can collect in the interests of public safety, for the purpose of protecting public health or for tax-related purposes; see ¶ 2.4 of the Code.

number of broad and ultimately non-exclusive purposes. In effect, with very few exceptions, the legislation empowers the authorities to obtain any type or amount of communications data they like and store that data forever.

33. In this respect, the powers granted under Part I closely resemble those that were at issue in *Liberty v the United Kingdom*, and which the ECtHR struck down as incompatible with Article 9.[20] Furthermore, the Part I regime lacks the limitations on the scope of collection, and the duration of storage, that were essential to the Court's decision to uphold RIPA's provisions pertaining to interception warrants for internal communications in *Kennedy v the United Kingdom*.[21]

34. It is therefore our view that the Part I regime violates Article 8, and that Parliament should amend the legislation so as to:

- Restrict the scope of collection of communications data obtained under Section 8(4) warrants to correspond with the targeting required of warrants under Section 8(1);
- Require that authorisations or notices for the collection or disclosure of communications data specify a single individual or set of premises to which that data must pertain (whilst defining 'premises' in a manner that precludes indiscriminate collection or disclosure);
- Require the destruction of communications data whose continued storage is not necessary or proportionate; and
- Restrict the grounds upon which the surveillance of communications data is available to those that are '*strictly necessary for safeguarding*' the UK's democratic institutions (to include the protection of public safety and the prevention of serious crime).[22]

III. The Secretary of State's virtually unlimited power to issue data retention orders violates Article 8 of the ECHR

35. Finally, we submit that the Secretary of State's powers under Section 1 of the DRIP Act to issue data retention orders that are not subject to any statutory limitations as to scale or scope, for up to 12 months, on any of the broad grounds found in Section 22(2) of RIPA, violate Article 8 of the ECHR.

---

[20] *Liberty and others*, *supra* n. 9, ¶¶ 64-70. Concerning the storage of data, see *Segerstedt-Wiberg and others v Sweden* (2006), ¶¶ 87-92.

[21] *Kennedy v the United Kingdom* (2010), ¶¶ 160 (distinguishing *Kennedy* from *Liberty and others* on the basis that for the interception of internal communications, '*the warrant itself must clearly specify, either by name or 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*', such that '*[i]ndiscriminate capturing of vast amounts of communications is not permitted*'), 162 (further distinguishing *Kennedy* from *Liberty and others* on the basis that where the interception of internal communications is concerned, '*any captured data which are not necessary for any of the authorised purposes must be destroyed*'), 164 (also noting the requirement of destruction of unnecessary data, and noting the additional requirement that '*intercept material [concerning internal communications] must be reviewed at appropriate intervals to confirm that the justification for the retention remains valid*').

[22] *See Rotaru v Romania* (Grand Chamber, 2000), ¶ 47.

36. We observe that under Section 1 of the DRIP Act, the Secretary of State has the power to issue, at her discretion, a data retention order that applies to any public telecommunications operator or class of operator, and that requires the retention of *all* data (or any subset of data). Moreover, she may issue such an order pursuant to any of the grounds set out in Section 22(2) of RIPA, including such additional grounds as she herself may establish via an order pursuant to Section 22(2)(h). Under the DRIP Act and the relevant provisions of RIPA, the term 'public telecommunications operator' can include any entity that offers a telecommunications (i.e. electronic communications) service to any substantial part of the public anywhere in the UK.

37. In other words, the Secretary of State may use any one of the broad and numerous grounds listed in Section 22(2) of RIPA for ordering virtually any provider of electronic communications services, from a local or national Internet service provider (such as British Telecom) to transnational companies such as Google, T-Mobile and Vodafone, to retain *all* communications data that it transmits or generates.

38. Even assuming that such a retention order would not have any validity outside of the UK's territorial jurisdiction (see the discussion at Part I above), the DRIP Act thus empowers the Secretary of State to order the indiscriminate retention of the communications data of the entire population of the United Kingdom.

39. The ECtHR has repeatedly made clear that the retention (or storage) of personal data constitutes an interference with the right to privacy, and must be necessary in a democratic society and proportionate to a legitimate aim in order to withstand scrutiny under Article 8.[23] In this context, the Court has specifically emphasised the requirement in its case-law that '*powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions*', and has closely examined whether the retention of data pertaining to an individual could '*be deemed to correspond to any actual relevant national security interests*'.[24]

40. The Court has also specifically emphasised that retention, as an interference with the right to private life, cannot be arbitrary if it is to comply with Article 8.[25]

41. In this respect, we note the CJEU's judgment in *Digital Rights Ireland* (see paragraph 20 above), in which the Court struck down the Data Retention Directive as violating fundamental privacy rights equivalent to those found in Article 8 of the ECHR. Part of the basis for the CJEU's decision was the fact that the Directive mandated the indiscriminate retention of communications data—including of individuals '*for whom there [was] no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime*'.[26]

---

[23] *E.g.*, *Leander v Sweden* (1987), ¶ 48; *Segerstedt-Wiberg and others*, *supra* n. 20, ¶ 73; *Rotaru*, *supra*
n. 22, ¶ 46.

[24] *Segerstedt-Wiberg and others*, *supra* n. 20, ¶¶ 88, 90; *see also Rotaru*, *supra* n. 22, ¶ 47; *Klass and others*, *supra* n. 16, ¶ 42.

[25] *Ibid.* at ¶ 76.

[26] *Digital Rights Ireland*, *supra* n. 8, ¶ 58

42. We therefore conclude that the power the DRIP Act confers upon the Secretary of State to issue indiscriminate (or otherwise non-individualised) data retention mandates constitutes a clear violation of Article 8 of the Convention, and that at minimum, Parliament should amend the legislation to provide that:
    - Any data retention order issued by the Secretary of State or her agents will only be valid with respect to data stored within the territorial jurisdiction of the UK (see Part I above);
    - The retention order may only require the retention of the communications data of a specific individual who is named in the order (as in a system of data preservation orders—see below), and the retention of whose data is strictly necessary in order to achieve one of the aims set out in Article 8; and
    - The order may only seek the retention of data of a type and amount that are proportionate to this aim.

43. We reiterate that these are the *minimum* changes to Section 1 of the DRIP Act (and related provisions of DRIP and RIPA) that Article 8 of the ECHR requires.

44. In order to ensure that interferences with privacy do not exceed what is necessary and proportionate, CDT has long urged national governments to adopt a regime of data preservation orders instead of data retention orders. Data preservation orders, which are used in the United States and (as CDT research in 2012 indicated) Japan, are issued by law-enforcement officials and require communications service providers to preserve data that is relevant to a specific investigation or proceeding.[27] In the United States, statutory law obligates communications service providers to preserve a user's data upon the request of a governmental entity pending the issuance of a court order or other process that compels disclosure.[28] Pursuant to the request, providers must preserve the relevant records for a 90- day period, which is renewable.[29]

45. These data *preservation* orders interfere with the privacy of only a small number of individuals, and do so in a targeted manner that is easily capable of meeting the necessity and proportionality (or non-arbitrariness) requirements found in the privacy provisions of international human-rights instruments. The UK's data *retention* orders, by contrast, could interfere with the privacy rights of many or all users of a provider's services and therefore run a much greater risk of being unnecessary or disproportionate.

46. We observe that the United States Congress has thus far declined to enact legislation permitting the issuance of data retention mandates, and that members of Congress have cited civil-liberties concerns in opposing draft legislation that would have created such mandates.[30] We encourage the UK Parliament to take a similar stance and uphold

---

[27] Center for Democracy & Technology, 'Introduction to Data Retention Mandates' (September 2012), *available at* https://www.cdt.org/files/pdfs/CDT_Data_Retention-Five_Pager.pdf.

[28] 18 U.S.C. § 2703(f)(1).

[29] 18 U.S.C. § 2703(f)(2).

[30] Greg Nojeim, 'Data Retention Hearing: Opposition from Both Sides' (13 July 2011), *available at* https://cdt.org/blog/data-retention-hearing-opposition-from-both-sides/; Mark Stanley, 'How the Data Retention Bill Impacts You – And What You Can Do About It' (27 February 2012), *available at* https://cdt.org/blog/how-the-data-retention-bill-impacts-you-—-and-what-you-can-do-about-it/.

fundamental rights by adopting a system of individualised data preservation orders rather than sweeping data retention mandates.

* * *

47. We hope this evidence will assist you as you undertake your review. Please do not hesitate to contact us if we can be of further assistance.

Sarah St Vincent
Human Rights and Surveillance Legal Fellow

October 2014

Jan Clements (Media Lawyer at The Guardian)

RIPA - proposed amendments to Serious Crime Bill and proposed RIPA code

Firstly, it is not clear why the RIPA proposals do not adopt the definition of 'journalistic material' set out in s13 Police and Criminal Evidence Act 1984 http://www.legislation.gov.uk/ukpga/1984/60/section/13. I am sure you are familiar with it, and it was commented on by Lord Justice Judge in R v CCC ex p Bright, Alton & Rusbridger 2000:

- para 117
- "Although this point was not closely addressed in argument, I shall return to the way in which journalistic material is defined in s13. The journalist must acquire or create the material for the purposes not of crime, but journalism. S13(3) is directed to the intention of the conveyor of the materials. If he intends that it should be used for journalism there is a rebuttable presumption that it was acquired by the recipient for that purpose. But if not, if for example, the recipient's purpose was to conceal evidence of a crime, the material is not journalistic material. In summary, if a journalist acquires material for the purposes of crime, or receives it other than for the purposes of journalism, it falls outside the ambit of s13(1). The objective of s9 is to enable the police to obtain journalistic material in the possession of a journalist, which is relevant to the criminal activities of others, including the individual who provided him with the material."

Instead, the RIPA proposals define 'journalistic material' narrowly as material that might *identify a source.* Similarly, judicial authorisation will only be required when the aim is to discover a source. The protection of the identity of a source is a crucial element of journalism, and an important part of freedom of expression.

However, confidential source information also includes information such as the very fact that the source has been in touch with a journalist, the location of the communications and the timing and frequency of such contacts. These elements of the communication between a journalist and a source are vital and the courts have recognised the need to protect them, even if a source's name is in fact in the public domain (indeed, this was so in the "Shayler" case of ex p Bright mentioned above).

It is well known that communications data can provide a wealth of information, apart from simply the identity of the parties. To provide adequate protection to journalism and freedom of expression, the amendments and Code should be based on the same definition of 'journalistic material' as in PACE, a tried and tested piece of legislation that has been in force for more than 30 years.

Secondly, applications for production orders under PACE are rarely used as an ex parte procedure, even in the most sensitive of cases involving national security and official secrets. (In fact I am not aware of any such ex parte applications). Yet there has been no damage to national security as a result of the notification given to the journalist or media organisation. It is not clear why a similar procedure (of giving notice) cannot be adopted in relation to RIPA. The fact that the RIPA application would be for intelligence gathering purposes and not necessarily for the investigation of a serious offence as in PACE does not seem a good reason.

February 2015

Paul Connolly (Readers' Editor, Belfast Telegraph)

It has come to my attention through my work as Readers' Editor of the Belfast Telegraph that Northern Ireland has not, and never has had, the Investigatory Powers Commissioner that is is bound to have by legislation (Section 61 RIPA). Please see p13 of the Surveillance road map published in August 2014 (attached for ease of reference).

The annotation in the booklet that "a recent Home Office exercise suggested that the public authorities which would come within the Northern Ireland Commissioner's remit use RIPA sparingly" has failed to re-assure. Indeed, the recent revelation by the Belfast Telegraph that the BBC in Northern Ireland uses RIPA to catch licence fee dodgers has also increased concern among both MPs and commentators like myself.

I know others have some responsibility over issues that may affect Northern Ireland, but in my long experience covering Northern Irish affairs (including a stint as Belfast Telegraph Security Correspondent) there is an imperative for local oversight for a wide range of reasons including its ongoing political history and historical questions of confidence in the administration of justice.

I would respectfully ask that the lack of appropriate structure in Northern Ireland form part of your review, so that this matter can be remedied.

I have appended below links to two of my recent columns that touch on this matter, and also the Belfast Telegraph report on RIPA and the BBC.

http://www.belfasttelegraph.co.uk/opinion/columnists/readers-editor/the-bbc-and-ripa-where-orwell-meets-the-office-30929733.html

http://www.belfasttelegraph.co.uk/opinion/columnists/readers-editor/northern-ireland-needs-a-snooping-commissioner-to-monitor-ripa-30688082.html

http://www.belfasttelegraph.co.uk/news/local-national/northern-ireland/bbc-uses-ripa-terrorism-laws-to-catch-tv-licence-fee-dodgers-in-northern-ireland-30911647.html

https://ico.org.uk/media/for-organisations/documents/1042035/surveillance-road-map.pdf

January 2015

Dr Andrew Defty and Professor Hugh Bochel
School of Social and Political Sciences, University of Lincoln

1. This submission deals primarily with the statutory arrangements for the oversight of investigatory powers by the intelligence and security agencies. It draws upon the findings of a major research project on parliamentary scrutiny of the intelligence and security agencies carried out at the University of Lincoln, which has been published in a number of journal articles and a book, *Watching the Watchers: Parliament and the Intelligence Services* (Palgrave, 2014). The research, which was funded in part by the Leverhulme Trust, examined the various mechanisms by which parliament and parliamentarians seek to scrutinise the intelligence and security agencies, including through legislation, debates, the work of the Intelligence and Security Committee and other parliamentary committees and the tabling of questions and Early Day Motions. In addition to a detailed examination of parliamentary business (reports, debates, EDMs and questions), the research drew on interviews with more than 100 MPs and Peers, including current and former members of the Intelligence and Security Committee, and with senior officials in the Foreign Office and the Cabinet Office. This submission also draws upon some on-going research on the impact of recent reforms on the operation of the Intelligence and Security Committee of Parliament.

The nature of intelligence oversight in the United Kingdom

2. Intelligence oversight is generally defined as a process of supervision designed to ensure that intelligence agencies do not break the law or abuse the rights of individuals at home or abroad. It also ensures that agencies are managed efficiently, and that money is spent properly and wisely, while some form of legislative oversight also helps provide democratic legitimacy for the work of the agencies. There is, however, no one model of intelligence oversight. It does, of necessity, vary from country to country, and may be affected and defined by a state's history, constitutional and legal systems, and political culture. Nevertheless, it is possible to identify a range of institutions and actors that may be involved in the oversight of intelligence and security agencies. Oversight is typically seen as taking place at several different levels: internal oversight at the level of the agency; executive oversight by the government; legislative oversight by democratically elected politicians, usually through specialist legislative oversight committees; external oversight by independent bodies such as the judiciary; and oversight by civil society through actors such as pressure groups and the media.

3. Britain has a patchwork of oversight arrangements involving different actors with different roles. Although these arrangements have evolved over time, statutory oversight is a relatively recent development. For most of their existence, oversight of the British intelligence and security

agencies was the sole preserve of government Ministers. Although the agencies have always been required to obtain warrants for interception of communications, the procedure for issuing warrants or for implementing interception was, until relatively recently, not subject to external review either by Parliament, the judiciary or any other body. From the mid-1980s a raft of legislation placed these arrangements on a statutory footing, and also established new oversight mechanisms with Commissioners to oversee the warranting procedure, a committee of parliamentarians to scrutinise the expenditure, administration and policy of the agencies, and an Investigatory Powers Tribunal to investigate complaints.

This submission deals with the statutory arrangements for oversight of the intelligence and security agencies by executive, legislative and judicial bodies within the UK.

Executive oversight – accountability to Ministers

4. Considerable attention has focused on the statutory role of the various Commissioners in providing a selective *post hoc* review of the warranting procedure for the interception of communications (see paras. 11-12 below). It is important to remember, however, that the first line in the accountability arrangements involves the review and signing of warrants by a senior government Minister. While the Commissioners only review a sample of warrants, all warrants for interception and intrusion by the intelligence and security agencies must be signed by a Secretary of State. Our research involved interviews with several individuals with experience of the warranting procedure, including serving and former Home and Foreign Secretaries. These Ministers frequently testified as to the robustness of the warranting process, the seriousness with which they approached the task, and the amount of time they devote to reviewing every single warrant.

5. However, the warranting process does raise a number of concerns. Firstly, it is a constitutional anomaly that warrants for the interception of communications and covert intrusion, actions which involve the state in the most serious intrusion of individual liberties, are signed by a government Minister and not a judge. Direct Ministerial responsibility for the actions of the intelligence and security agencies is an important safeguard. However, some form of independent legal review of the warranting process at the time at which warrants are signed, involving either a judge or an independent inspector general would significantly strengthen the oversight procedures. **If changes were made to the statutory arrangements for the issuing of warrants consideration might be given to the involvement of some form of external legal scrutiny *alongside* the role of Ministers in the issuing of warrants.**

6. The process of having warrants signed by a Secretary of State also raises questions about the

level of scrutiny applied to each warrant. While those involved claim to spend a considerable amount of time reviewing warrants the process must be extremely demanding. Questions are often raised about the extent to which the Commissioners, whose role is only part-time, can provide effective review of only a sample of warrants, (see para. 12 below). Yet those Ministers responsible for signing *all* warrants must combine this with running a large government department, being a senior member of the government, and other parliamentary and constituency duties. **An additional layer of independent judicial scrutiny at the point at which warrants are signed may help to relieve the burden on hard–pressed Ministers and provide more effective scrutiny of the process.**

7. Another question relates to who signs warrants for interception in the absence of the designated Secretary of State. The legislation states that warrants must be signed by a Secretary of State. Although the assumption is that this will be either the Home or Foreign Secretary, the legislation does not specify in detail which Secretary of State, or who should sign in the absence of the relevant Minister. As part of our research we interviewed a Secretary of State from another department entirely, with no experience in the Home Office or of dealing with the intelligence and security agencies, who claimed to have routinely signed Home Office warrants when the Home Secretary was unavailable. In order to ensure that the arrangements for issuing warrants is robust it would be helpful if legislation specified in more detail who should sign warrants and what the process should be in the absence of the designated Secretary of State. **It would be preferable if, in the absence of the appropriate Secretary of State, a clear chain of responsibility was established which involved passing warrants to another designated Secretary of State, or upwards to the Prime Minister, rather than to a Secretary of State from any other department.**

Legislative oversight – the Intelligence and Security Committee of Parliament

8. The Intelligence and Security Committee (ISC) is a statutory committee established by the Intelligence Services Act 1994, to examine the administration, policy and expenditure of the three intelligence and security agencies. The anomalous status of the ISC led to considerable debate and repeated questions in Parliament about the independence of the Committee. Significant reforms included in the Justice and Security Act 2013 reconstituted the ISC as a parliamentary committee, expanded its remit to encompass the wider intelligence community, and also provided new powers to oversee operational issues and request access to information. The resources available to the ISC have also increased considerably since 2010. Although the ISC does not have a direct role in approving the interception of communications it is responsible for overseeing the administration, policy and operational practices of the intelligence and security agencies. It is therefore central to the effective oversight of the use of investigatory powers by the agencies.

The increased powers and additional resources now available to the ISC are a welcome development. Although it remains to be seen whether the reformed ISC will in practice enhance the current oversight arrangements, it would be premature to recommend further statutory reform of the ISC at this time.

9. Nevertheless, some changes to the way in which the reconstituted ISC operates may serve to further enhance its credibility, most notably in relation to the membership of the Committee. It is widely accepted that the legitimacy of legislative intelligence oversight bodies is enhanced if they are chaired by a member of an opposition party. This is a model which has been followed in a number of other states, and one which has periodically been discussed in relation to the ISC. The profile of others members of the Committee may also have a significant impact on the perception of the Committee, both in Parliament and beyond. A large proportion of those who have served on the ISC have previously held Ministerial office (22 out of 37 current and former members). The limited profile of the membership, and in particular the reliance on parliamentarians with existing experience of working with the agencies, means that the ISC has done little to broaden the pool of parliamentary knowledge and understanding of intelligence. Moreover, while the tendency towards seniority in appointments to the ISC may have enhanced the Committee's standing with the agencies, it has done less to convince Parliament that the Committee is capable of rigorous and independent scrutiny. **Changes to the composition of the ISC, including the practice of appointing a Chair from an opposition party, coupled with a more bold approach to the appointment of members who may be viewed as more independent, would help enhance the ISC's credibility in Parliament and beyond.**

10. Another potentially significant improvement in the current arrangements would be an increase in the level of cooperation between the ISC and other bodies involved in oversight. As noted below (para. 13), cooperation between oversight bodies is an important means of avoiding accountability gaps. There have, however, been significant barriers to cooperation between the ISC and the Commissioners and the Investigatory Powers Tribunal (IPT). Since 1994, the ISC has met on an annual basis with the Commissioners responsible for overseeing the warranting procedure for the intelligence and security agencies. However, despite repeated requests the ISC only met representatives of the Investigatory Powers Tribunal for the first time in 2010. The ISC has also repeatedly been denied access to the confidential annexes to the Commissioners' published reports. The ISC first requested access to the confidential annexes in 1998, and continued to do so over the following years, most recently in its annual report for 2010-2011, but access has continued to be denied. **Cooperation between the various oversight mechanisms is central to ensuring that policy and operations are in concert and that accountability gaps do not emerge. Steps should be taken to allow for greater and more substantive**

cooperation between the ISC, the Commissioners and the IPT, including access to each other's procedures and unredacted reports.

Judicial oversight – The Commissioners and the Investigatory Powers Tribunal

11. The process of reviewing the authorisation of warrants for interception and intrusive investigations by the intelligence and security agencies is carried out by the Interception of Communications Commissioner and the Intelligence Services Commissioner. The structural limitations on the work of the Commissioners are well known and will no doubt feature heavily in a number of responses to this consultation. These concerns do not relate to the quality of the individuals holding the office of Commissioner, all of whom have held high judicial office, but to the nature of the post and the timing of review. Perhaps the most significant limitations relate to the fact that the Commissioners operate on a part-time basis and only review a relatively small sample of warrants. Moreover, the process of review is *post hoc*, with the result that mistakes are only identified after a potential infringement of liberties has taken place. In the course of their work the Commissioners do routinely identify mistakes and provide for restitution. However, if mistakes are identified in a sample of warrants then further, possibly many more, mistakes must go undetected in the warrants that are not subject to scrutiny. It is important to remember that every warrant involves a potential breach of human rights, with potentially significant consequences. It is also important to remember that oversight mechanisms which identify mistakes also serve to enhance the efficacy of the agencies. **The *post hoc* nature of the Commissioners' work, and even the more selective approach, would be more acceptable if some form of independent judicial review were provided at the stage at which warrants are signed (see para 5). In the absence of this, the scale and seriousness of the work of the intelligence and security agencies, and the commensurate demands on those responsible for oversight, is such that a more comprehensive and robust system of review should be instituted, whereby many more, if not all, warrants should be subject to review.**

12. The demands on the Intelligence Services Commissioner, in particular, have increased in recent years. In addition to the Commissioner's role in overseeing the warranting process, the Justice and Security Act expanded the role of the Intelligence Services Commissioner to include, at the Prime Minister's request, keeping under review 'any aspect of the functions of ' the intelligence services, the heads of the intelligence services, and any part of the armed forces engaged in intelligence activities. Not only does this new and expansive role place an extra burden on the resources of the Intelligence Services Commissioner, it also appears to overlap somewhat with the functions of the ISC. The lack of clarity about roles can, of course, lead to duplication but may also lead to accountability gaps if each body assumes that the other has primary responsibility in a particular area or case. There is also the possibility that governments

can play scrutiny bodies off against each other, assigning tasks to the body that they assume will offer the most agreeable response, or when duplication occurs, being able to pick and choose which findings to accept. **While ensuring close cooperation between the various oversight**

bodies, it would nevertheless be beneficial if a clear demarcation was maintained between their respective roles, and in particular if some clarity was provided in relation to the overlapping statutory roles of the ISC and the Intelligence Services Commissioner.

Cross-cutting issues

13. The regulatory framework: As noted a number of times in this submission (paras. 3, 10, 12) there are a number of bodies involved in the oversight of the intelligence and security agencies. This multi-faceted approach has several advantages. A combination of organisational and functional oversight serves to overcome the potential accountability gaps when oversight arrangements are tied to the activities of specific agencies. A combination of Executive and legislative scrutiny is an important check on Executive power, and the use of external review processes, including by judges, not only helps ensure that intelligence agencies operate within the law, but may also help to lift oversight above political partisanship. However, there are also a number of potential problems with what may be seen as a patchwork approach to intelligence oversight. It is important to ensure that as changes take place within the intelligence community, both organisationally and functionally, oversight mechanisms are adapted to keep pace with such changes and that gaps do not emerge in the oversight system. It is also important to remember that each level of oversight has a distinct and important role in terms of providing effective and credible oversight, and that changes in the role and powers of one level of oversight may not compensate for deficiencies at another level. Strong Executive control does not obviate the need for parliamentary scrutiny, and wider parliamentary oversight of the efficacy of intelligence agencies and operations does not preclude the role of the judiciary in addressing questions of legality. **In considering reform of any aspect of the regulatory framework consideration should be given to the framework as a whole to ensure that accountability gaps do not emerge. It should also be appreciated that the breadth and depth of oversight are likely to be enhanced if there is a good level of cooperation between the various actors involved.**

14. Openness and transparency: The work of the intelligence and security agencies is of necessity secret. However, the work of intelligence oversight bodies should wherever possible be open and transparent. It is not sufficient that oversight should take place, if oversight bodies are to have legitimacy then oversight should, to some degree, be seen to be taking place. With regard British intelligence oversight bodies, this has not always been the case. There has been considerable progress in recent years with, for example, the ISC, the Commissioners and the IPT

establishing a web presence, and since 2010, the ISC in particular has developed a more outward facing profile. However, there is little evidence for widespread knowledge and understanding or indeed confidence in the regulatory framework under which the agencies operate, and the roles and processes of the Commissioners and the IPT in particular, remain

somewhat opaque. Our research indicated that even within Parliament there remains considerable uncertainty not just about the roles but the very existence of the various oversight bodies. **Continued efforts should be made on the part of *all* the statutory oversight bodies to enhance their public profile, explain their work more widely both to the public and to Parliament, and engage more closely with others involved in scrutiny both in Parliament and civil society.**

Conclusions & Recommendations

Executive Oversight – accountability to Ministers

A. If changes were made to the statutory arrangements for the issuing of warrants consideration might be given to the involvement of some form of external legal scrutiny *alongside* the role of Ministers in the issuing of warrants.

B. An additional layer of independent judicial scrutiny at the point at which warrants are signed may help to relieve the burden on hard–pressed Ministers and provide more effective scrutiny of the process.

C. It would be preferable if, in the absence of the appropriate Secretary of State, a clear chain of responsibility was established which involved passing warrants to another designated Secretary of State, or upwards to the Prime Minister, rather than to a Secretary of State from any other department.

Legislative oversight – the Intelligence and Security Committee of Parliament

D. The increased powers and additional resources now available to the ISC are a welcome development. Although it remains to be seen whether the reformed ISC will in practice enhance the current oversight arrangements, it would be premature to recommend further statutory reform of the ISC at this time.

E. Changes to the composition of the ISC, including the practice of appointing a Chair from an opposition party, coupled with a more bold approach to the appointment of members who may be

viewed as more independent, would help enhance the ISC's credibility in Parliament and beyond.

F. Cooperation between the various oversight mechanisms is central to ensuring that policy and operations are in concert and that accountability gaps do not emerge. Steps should be taken to allow for greater and more substantive cooperation between the ISC, the Commissioners and the IPT, including access to each other's procedures and unredacted reports.

Judicial oversight – The Commissioners and the Investigatory Powers Tribunal

G. The *post hoc* nature of the Commissioners' work, and even the more selective approach, would be more acceptable if some form of independent judicial review were provided at the stage at which warrants are signed (see para 5). In the absence of this, the scale and seriousness of the work of the intelligence and security agencies, and the commensurate demands on those responsible for oversight, is such that a more comprehensive and robust system of review should be instituted, whereby many more, if not all, warrants should be subject to review.

H. While ensuring close cooperation between the various oversight bodies, it would nevertheless be beneficial if a clear demarcation was maintained between their respective roles, and in particular if some clarity was provided in relation to the overlapping statutory roles of the ISC and the Intelligence Services Commissioner.

Cross-cutting issues

I. In considering reform of any aspect of the regulatory framework consideration should be given to the framework as a whole to ensure that accountability gaps do not emerge. It should also be appreciated that the breadth and depth of oversight are likely to be enhanced if there is a good level of cooperation between the various actors involved.

J. Continued efforts should be made on the part of *all* the statutory oversight bodies to enhance their public profile, explain their work more widely both to the public and to Parliament, and engage more closely with others involved in scrutiny both in Parliament and civil society.

October 2014

Demos submission to the Investigatory Powers Review: attitudes to privacy and new forms of oversight

1.1 This document is divided into two sections. Part 1 sets out current attitudes to online privacy in so far as it might affect surveillance legislation. Part 2 sets out a small number of specific suggestions for how to improve the current oversight regime.

1.2 Neither section is comprehensive, but rather initial thoughts and analysis on the subject.

Section 1: internet privacy

1.3 UK citizens recognise that sharing information is an increasingly important part of modern life. Certainly, most of us accept that both private and public bodies – from Tesco through its Clubcards to Amazon, Oyster and Google – learn and record a vast amount about us daily.

1.4 When we want to find something, we search online: Google Search now has around 30 million unique UK visitors each month.[1] When we shop or bank, we increasingly do that online, too – 73 per cent of people with internet access at home use it to purchase goods online, while almost two-thirds use online banking services and social networking sites.

1.5 New technology is also encouraging new ways to share information: 39 per cent of phone users have smartphones, compared with 27 per cent a year ago, which has resulted in a growth in what is known as location data.[2] One of the reasons we now share more data is because there are considerable benefits in doing so. Providing personal information and behavioural data can result in services and applications that are more tailored to users' needs, for example an improved shopping experience when buying goods online, better network coverage, greater security when online, and free applications and services.[3] According to Ofcom, almost six in ten people think new communication methods have made their lives easier – whether through using online banking; having a better, more tailored shopping experience by buying goods online; or through the provision of improved services in general.[4]

1.6 These necessities of modern life are resulting in changes in what we consider personal or public. McKinsey Global Institute has calculated that 30 billion pieces of content are shared on Facebook each month, many of them personal.[5] With the likely advent of the so called 'internet of things', increased broadband speeds and the falling cost of storage and devices – these trends are highly likely to continue.

1.7 As sharing information becomes an increasingly important part of modern society, attitudes about personal information and behavioural data also evolve. This too is

likely to remain in flux. It is better to view attitudes to specific platforms or data and privacy as a constantly shifting.

1.8 The Eurobarometer survey *Data Protection in the European Union: Citizens' perceptions* has asked European citizens – including UK citizens – periodically about their views on data protection. In 2003, 60 per cent of UK respondents were concerned about data protection; this figure rose to 68 per cent in 2008. In 2003, 73 per cent of UK respondents said were concerned about leaving information on the internet more often than before, and this figure had increased to 79 per cent by 2008. Furthermore, the poll has found a large increase in the number of people in the UK who think current legislation is unable to deal with personal information on the internet.[6]

1.9 What people consider to be private or personal information ; and what worries them about data privacy is important for any discussion of surveillance, since the general principle in respect of surveillance is the more private information is, the greater the likely harms involved with third party access, and therefore the higher degree of authorisation (and more limited the purposes) should be required. We consider this to remain an important principle to maintain**.** There have been a number of surveys which examine changing attitudes toward privacy in relation to digital or internet data and behaviour which can help inform any decisions made in regard to future legislation. We summarise them below.

What is private today?

1.10 While it might be argued that attitudes about whether an individual's home is private are relatively clear, it is less clear in respect of online data. This is one reason the debate about online surveillance has been difficult to resolve.

1.11 In one Eurobarometer poll, a bare majority of UK respondents considered photos of themselves to be personal data, less than half considered 'who your friends are' to be personal data, 41 per cent thought that details of the websites they visit were personal data, and only 32 per cent thought their tastes and opinions were personal data, yet in contrast, large majorities regard financial data as personal.[7]

1.12 In a representative poll of 5,000 members of the public (Great Britain), when asked if people thought certain types of information were personal, there was a clear difference between 'personal information' and 'behavioural data'.

- 83 per cent believe health records are personal
- 45 per cent believe current location is personal
- 29 per cent believe favourite websites is personal[8]

1.13 In general terms, the public tends to consider information that might allow someone to be personally identifiable or details about their personal lives – such as phone numbers or how many children one has – as personal.

1.14 By contrast, the public tends to view information about behaviour – often generalisable or aggregatable – as less personal: 45 per cent of the public believes that your current location is personal, and only 30 per cent agree that information about the products and services you buy is personal. Different segments have highly diverse views, however.

Concerns about data access and use

1.15 Although the subject is still in a state of flux – it is a quickly moving field – there is a significant trust deficit when it comes to personal data.

1.16 According to the 2014 Deloitte Data Nation report, the majority of people place more trust in both public healthcare providers and other public sector bodies with their personal information than in commercial organisations. Fifty one per cent trust public sector organisations (not including healthcare providers – which is even higher); compared with 34% who trust internet service providers and 31 % who trust social media organisations. That said, 24% of people in the UK do not trust any type of organisation with their personal information.

1.17 According to a recent poll by Ipsos-Mori and the Royal Statistics Society (2014), only between 4 and 7% of respondents say they have a high level of trust in institutions such as media, internet companies, telecommunications companies and insurance companies to use data appropriately. Similarly to the above, 36% trust the NHS, and 41% trust their GP. Similar to the survey above, internet companies are not trusted by 54% on using data (32% do not trust them generally).

1.18 Chief concerns surrounding personal information sharing tend to relate to two specific sets of issues:

- not knowing how and why personal data are being collected
- losing control over what happens to it, who has access to it and what they do with it

1.19 **We believe that the concerns relating to privacy is not that principally that data are being collected, as this is increasingly accepted as a part of modern life. Rather, citizens are highly concerned about data being misused.** We call this ‘control loss’ – as it is predominantly about the individuals losing control over their information, rather than the fact of actually sharing it *per se*.

1.20 Research shows that the public is increasingly aware that information is collected, but not clear about how. The ways in which people's personal information are collected and shared are sophisticated; this can be done in ways that the individual might not reasonably expect or even understand.

1.21 The second aspect of control loss relates to *who* has access to personal information and what they do with it. One 2011 poll showed that nine out of ten consumers in the UK would like control over the personal information they share with companies and the manner in which it is stored.[9] Other research supports this position; the Information Commissioner's Office (ICO) found that six in ten 'feel they have lost control over the way their information is collected and processed'.[10]

1.22 Third party access ranks among people's highest concerns about information sharing, especially when it is used for targeted advertising. Nearly half (48 per cent) of UK adults say they are not comfortable with websites using their information in this way (which contrasts with a more positive attitude to companies using personal information to generate more business or develop new services).[11] This survey also found that the loss of personal data to unknown third parties 'was less acceptable than companies using the information themselves'.[12] Consumer Empowerment Tracker research from 2011 found that nine out of ten consumers believe that they should 'be able to control what information organisations collect about me and what they use this information for'.[13]

1.23 Both the Deloitte and Ipsos survey find similar results in terms of people's concerns. According to the Ipsos survey (2014) two of the three worst things a company can do to make someone stop using the company are to lose personal data (72%) or to sell anonymous data about its customers to other companies (63%) – more than choose exploiting foreign workers (37%), protecting the environment (35%), or even charging more than their competitors (53%). According to the Deloitte poll (2014), 64% of people are concerned about the sale of anonymised date (to the extent that they would be likely to stop transacting with companies engaging in this practice). This number has gone up from 56% two years ago.

1.24 Interestingly, 64% of consumers either don't mind or are happy to share their personal information if it leads to direct benefits in the form of financial savings, product or service improvements, guidance to meet personal goals, or receiving a personalised product or service. Even those who are most concerned about organisations having access to their personal information are more inclined to share their personal data in exchange for benefits.

Fragmentation of attitudes

1.25 As noted above one of the most important trends has been a fragmentation of what it is that people consider to be private or public. In a recent Eurobarometer poll, a bare majority of UK respondents considered photos of themselves to be personal; less than half considered 'who your friends are' to be personal; 41 per cent thought that details of the websites they visit were personal; and only 32 per cent thought their tastes and opinions were personal. In contrast, large majorities regarded financial data as personal.[14] Nevertheless, around two-thirds of those banking online or visiting government websites said they 'are happy to enter their personal details', and just over half of people shopping online said that 'they are happy to do so'.[15]

1.26 Importantly, these figures vary according to the experience, age and demographic of the user. Ofcom's annual survey on internet use and attitudes shows significant differences by age and socio-economic groups, an example being that those in the younger online demographic are more likely to feel more confident using online services.[16]

1.27 A 2012 Demos pamphlet 'Data Dialogues' based on a survey of 5,000 British adults, found that, although there are some broad areas of agreement, what constitutes 'personal' information often varies from person to person. The public falls into one of five categories each characterised by a distinct set of views about personal information:

- *Around 30 per cent of the population are 'non-sharers'.* They are knowledgeable about data protection, view much of their data as personal and take measures to protect it.
- *Around 22 per cent of the population are 'sceptics'*. They do not have a single view about whether data are personal or impersonal – but they are sceptical about whether or not government and companies can be trusted. Unlike the non-sharers, they do not use online services much. They share data and information if the personal benefits of doing so are clear to them, but they want measures to give them simple, direct and regular control over their data.
- *Around 20 per cent of the population are 'pragmatists'.* They do not know all the details of how their data are used, but take small measures to protect their privacy. They prefer efficient services to complete privacy.
- *Around 19 per cent of the population are 'value hunters'.* They understand the value of their data, and the benefits of sharing it. They are not overly concerned about risks to personal information being shared – but want to get the most in return.
- *Around 8 per cent of the population are 'enthusiastic sharers'.* They categorise a lot of their information as impersonal, and subsequently are comfortable with sharing it. They are amenable to sharing more information in future, but are concerned about the ways in which those data could be misused.

1.28 On the whole, the youngest generation of consumers (15 to 24) are more trusting of organisations and concerns about organisations having access to personal information tend to increase as people age (Deloitte, 2014). Similarly the appetite to exchange personal information for tangible benefits varies considerably with age: 32% of consumers in the UK aged between 15 and 24 are happy or don't mind exchanging personal information for a range of benefits, including save money on products/services, prove products/services, receive guidance to meet personal goals and receive personalised products/services; whereas only 15% of consumers in the UK aged 65+ are happy or don't mind.

Lack of awareness

1.29 Knowledge about the general principles of data use is fairly widely known. For example, 85 per cent are aware that online purchasing history data are collected and used, and 81 per cent are aware of supermarket loyalty schemes. Knowledge about G-mail-based advertising is lowest, although over two-thirds (67 per cent) of the public are aware of it

1.30 However, people know and understand less about the specific ways in which personal information is collected and used. One good example is the way 'cookies' are collected and stored. Cookies allow pages like Facebook to divert traffic onto their partners' websites. A survey conducted by PricewaterhouseCoopers LLP found that only 13 per cent of respondents fully understood how cookies worked, although 37 per cent had heard of them.[17] Similarly, Ofcom's *Adults Media Use and Attitudes Report* found that just over half (53 per cent) knew how to delete cookies from a PC, laptop, netbook or tablet website browser.[18] The Communications Consumer Panel (CCP) – an independent group of experts that provides advice to Ofcom – found that there was less awareness that mobile phone apps can also collect personal data (45 per cent knew they did).[19]

1.31 More prosaically, privacy and data-sharing agreements are sometimes non-existent, misleading, or overly technical and jargon-ridden, which makes them difficult to understand. The CCP argued in 2011 that companies need to improve consumers' awareness of how their data are collected and used, and provide straightforward information for them. Although the majority of people are aware of website terms and conditions, most of us barely or never read when downloading apps or uploading information.[20] As a result, consumers may not be making informed decisions about withholding their data and protecting their privacy, or sharing data and obtaining benefits.[21]

1.32 According to Deloitte (2014) Almost half 45% of adult internet users in Britain admit to always or fairly often agreeing to the terms and conditions and/or privacy polices of online services they sign up to without reading them. And 48% of smartphone users admit the same when they download mobiles apps. Deloitte's analysis of privacy policies from the top 100 websites visited by UK internet users

found that, on average, an adults would need to spend 26 minutes reading through a single policy to comprehend the content. According to this survey, only 34% of adult internet users agree that privacy policies are clear about how companies intend to use their data. Even worse, this falls to just 22% among those who actually read the fine print.

Section 2: citizen involvement in surveillance oversight

2.1 Our judgement is that citizens on the whole are content for their data to accessed (especially by government agencies who are more trusted on the whole than private companies) but want to ensure that a) some public benefit accrues from that; and b) that where there is possibility of misuse (in the ways set out above) there is a strict oversight and scrutiny system.

2.2 As it stands, the oversight regime is necessarily complex, both multi-Act and multi-agency. Commissioners, Parliamentarians, Ministers, and law enforcement agencies themselves all form the machinery and participate in the process of oversight as defined by a number of interlocking legal and regulatory structures. There are a number of technical, and procedural questions related to the robustness and independence of this regime. Critics have pointed to, amongst other things, inter-agency sign-off, a lack of Parliamentary accountability for Ministerial warrant, and the executive nomination of members of the Intelligence and Security Committee as areas of particular need for reform.

2.3 However, another vital, enabling attribute of a robust oversight regime is the understanding of that regime by the public, and their trust and involvement within it. Britain's National Security Strategy recognises that security and intelligence work in general is predicated not only on the public's consent and understanding, but also on the active partnership and participation of people and communities.[22] Serious and recognised damage to security occurs when the state's efforts are not accepted or trusted. It is not enough for surveillance to be overseen, but for it to be recognized and accepted that it is overseen. This section sets out some suggestions for how that might be best achieved.

2.4 The key question is how to establish trust in surveillance oversight. This question sits within a wider, decades-long process whereby Government activity – across many areas of its business – has become more open and transparent. This agenda has been deliberate attempt to make Executive action more porous, participatory and its work better understood.[23] Service users, interest groups, community leaders, professional bodies, charities and NGOs are now routinely involved in open policy-making and practice.[24] Official data has, likewise, been moved into the public domain for public scrutiny and use.[25]

2.5 But public trust is something it is increasingly harder for public institutions to get and to hold. Ipsos MORI's 2011 'veracity index' found that, on average, 61% the police, less than half trust Civil Servants, and just 19% Government Ministers.[26] Trends in which professions tend to be most and least suggests that regular, personal contact might play a role: doctors and teachers are the most trust professions (89% and 86% of us, respectively, trust them to tell the truth), and politicians and journalists the least (21% and 18% respectively on the same measure).[27]

2.6 Demos recognises that intelligence and security work is intrinsically difficult to make either accessible to non-governmental actors, or to make more public. The 'sphere of secrecy' that has surrounded this kind of work is rationally imposed for legitimate reasons. Active operations can be undermined by breaches to their security, security personnel can be personally endangered by public exposure, and sources and methods can become less effective, or not effective at all, if they are publicly known.

2.7 However, we believe that any review of Britain's oversight regime must consider new ways of responsibly increasing citizen participation and trust in that regime. We believe two broad kinds of reforms are plausibly able to deliver both greater public trust, without undermining the vital work of law enforcement agencies.

- **Public understanding:** or lifting information, principles and context outside of the 'sphere of secrecy'. New structures, processes and opportunities to increase the public understanding of intelligence work, the threats that they counter, the overall trade-offs that need to be made and the balances that are struck.

- **Citizen involvement:** or lifting members of the public or civic society into the 'sphere of secrecy'. It may also be possible to directly involve citizens in the oversight process, and to facilitate interactions between citizens and the oversight regime that serves them.

2.8 We lay out a number of opportunities below, for consideration:

2.9 First, clear, public-facing communications on the nature and type of Britain's current oversight regime. This could include:

- Interventions must be considered which increase and allow public understanding of the oversight regime, and how it operates to balance incidences of interference of privacy with the public interest.

- Accessible, jargon-free, non-technical literature should be created and shared by Government to map out the organizations, individuals, processes and

structures involved in oversight, and how they are involved. This should include accessible descriptions of the relevant legislation, and practical scenarios of how they are implemented.

- Government should consider working with media organizations to both produce and disseminate this content. This could include video and infographic descriptions. The content should be de-politicised, and cross-Partisan, and involve a range of actors in its dissemination, including the Government and its critics. There is a clear public interest in increasing public awareness of the reality of this policy area, and all reasonable, responsible actors in the debate have a responsibility to work together to disseminate clear, informative content to interested citizens.

- There should also be clarification of how RIPA has been interpreted, and how it is being applied. A number of secondary-level interpretations of RIPA have been made (sometimes referred to as Guidance Notes), and these have not always been publicly explained. This is concerning, given the recognised role of civic society and academia in scrutinising public legislation and executive practice. To enable this, it is important that the practical reality of current legislation be made, and include broad in-principle, hypothetical explanations of the scenarios wherein RIPA is used.

2.10 Second, there should be further interventions to better explain the role and nature of intelligence work

2.11 The work and role of intelligence agencies must, likewise, be better understood both by the public in general, and by the NGOs, commentators and academics active in the debate about privacy, oversight and surveillance. We believe much of this debate has been unhelpfully polarised and unconstructive as the result of a lack of accepted, legitimate, recognised opportunities for intelligence agencies to publicly and responsibly communicate the changing realities and pressures they confront in keeping Britain safe and responding to a constantly changing series of threats. This could include:

- Routine, de-politicised, evidence-based assessments of vulnerability and risk. The current terrorism threat-level regime provides little contextualising information about the nature or scale of threats the UK faces. Public statements that have been made on security risks have been occasional, irregular, and often closely precede or follow a party-political announcement or policy roll out. An independent, authoritative voice should be established to publicly communicate security threats.

- Increase the number of intelligence personnel that can be publicly identified and can publicly account for the activities of their respective agencies. Only a very small number of very senior standing intelligence officers are publicly identified, and can account and explain for the activities of their agency. This

necessarily makes their appearances infrequent, very high-level, and often only in the context of a perceived controversy or crisis. Whilst many members of each agency cannot be made publicly identified, we believe that a greater number could be, without operational risk. This would allow a greater number of more routine interactions, both in public, open-door Parliamentary sessions and directly with civic society.

- Community engagement of intelligence. Police Constabularies have established a number of community outreach programmes to attempt to strategically alter how they understand and interact with key stakeholders. For example, the Metropolitan Police Service Communities Together Strategic Engagement Team (CTSET) regularly engages with a number of community groups, especially at times of heightened tension.[28] A review of these attempts has found positive evidence that they increase feelings of safety, and improve police community relations and community perceptions.[29] It should be considered whether principles and strategies from this area can also be used by intelligence agencies, not for the purpose of gathering intelligence, but to form community bonds, increase trust and improve understanding.

- Public Q&A sessions between members of law enforcement agencies and the public. A first step to establish better ways for the intelligence agencies to explain their role in keeping Britain safe could be to establish a recognised and legitimate forum whereby members of the public can ask them questions and be provided with more information.

2.12 *Third, there is an opportunity for more direct involvement from citizens and civic society as part of the oversight regime.*

2.13 At the heart of the legal infrastructure governing oversight – especially RIPA - are three animating principles: proportionality, necessity and legitimate aim. It is these principles that the machinery must protect and enforce, and be seen to protect and enforce.

2.14 The principles of 'necessity' and 'legitimate aim' are fairly easily defined within an operational context. The question of whether a given body of information is needed for a defined statutory purpose, whether it can be collected using less intrusive means, and whether any given act of intrusive act of surveillance is likely to supply that information can, broadly, be defined, justified and assessed by subject matter experts.

2.15 Proportionality however is less easily defined. This discrimination is made by balancing the seriousness of the intrusion into the privacy of the subject of the investigation against the need of the activity in investigative terms.[30] This discrimination demands a much broader assessment of the intrusion within the context of the case, but also an assessment of the case within a broader societal context.

2.16 We believe that the assessment of proportionality is neither a technical nor technocratic process. In the context whereby privacy is less clearly understood, different people, with different backgrounds, life experiences and beliefs will take legitimately different positions on whether some acts of intrusive surveillance or proportionate.

2.17 We therefore suggest that steps should be taken to broaden the backgrounds and experiences of those that are able to contribute to the oversight of whether a judgement about a given interference with privacy is proportionate or not. A wider body of voices must be heard in this assessment in order to insure that the assessment of proportionality reflects society's changing view of what is private. Specifically this could include the following:

- We suggest an effective way to do this would be the creation of a new structure: **the surveillance jury.** Juries have been shown to be one of the most trusted institutions.[31] Involves people in process purely because they do not need to satisfy a specialist or professional qualifying criterion. A Surveillance Jury – of randomly selected members of the public should sit alongside other oversight structures to produce *post-hoc* advice on a small number of selected cases of intrusive surveillance, randomly selected for review. It should be supported by other oversight bodies, and a small technical secretariat of experts, to assess whether, in each case, the interference with privacy was a proportionate one. The role of the Surveillance Jury would be as a 'pressure gauge' to ensure that the expert, Parliamentary and intra-agency assessments of proportionality accord with the public's assessment of proportionality. It should have no direct power to block or censure the activities of the intelligence agencies, and should only provide strategic, broad assessments. However, it would be the responsibility of other oversight bodies to recognise the views of this body, and to include them in their own assessments and communications, such as the Annual Reports of the Interception Commissioner to the Prime Minister.[32]

- A further element of this additional involvement is ensuring some degree of involvement of civic society in intelligence oversight. It is important that independent, responsible members of civic society can better understand the practical pressures and daily trade-offs of intelligence work. Embedding liberty campaigners in police command centers during the policing of demonstrations has worked well.[33] Subject to agreements around what can and cannot be published, this has allowed the presence of informed, independent commentary of police action. A similar arrangement should be considered to embed members of civic society within intelligence agencies. An enabling agreement can be established that can protect the agencies from damage to their sources and methods, whilst protecting the genuine independence and capacity for criticism of independent observers.

End.

Jamie Bartlett
Carl Miller

December 2014

[1] Ofcom, *Communications Market Report 2012,* July 2012

[2] Ofcom, *Internet Use and Attitudes: 2012 Metrics Bulletin*, July 2012, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/2012_metrics_bulletin.pdf (accessed 8 Aug 2012)

Ofcom, *Communications Market Report 2012,* July 2012

[3] Communications Consumer Panel, *Online Personal Data: The Consumer Perspective 2011*, www.communicationsconsumerpanel.org.uk/Online%20personal%20data%20final%20240511.pdf (accessed 21 Aug 2012)

[4] Ofcom, *Communications Market Report 2012*, July 2012

M. Wind-Cowie and R. Lekhi, *The Data Dividend*, London: Demos, 2012, www.demos.co.uk/files/The_Data_Dividend_-_web.pdf (accessed 9 Aug 2012)

[5] S. Sengupta, 'Zuckerberg's unspoken law: sharing and more sharing', *New York Times*, 23 Sep 2011, http://bits.blogs.nytimes.com/2011/09/23/zuckerbergs-unspoken-law-sharing-and-more-sharing/ (accessed 17 Apr 2012)

[6] European Commission, *Data Protection in the European Union: Citizens' Perceptions*, European Commission Analytical Report, Eurobarometer 225, Feb 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf (accessed 13 Aug 2012)

[7] European Commission, *Attitudes on Data Protection and Electronic Identity in the European Union*.

[8] J. Bartlett, *Data Dialogue,* 2012

[9] Ctrl Shift, *Tracking the control shift*, Briefing Report, 2011

[10] SMSR and ICO, *Report on the Findings of the Information Commissioner's Office Annual Tract 2011 – Individuals*, Social and Market Strategic Research and the Information Commissioner's Office, Oct 2011.

[11] Ofcom, *Adults Media Use and Attitudes Report*, 2012, http://tinyurl.com/czbzovo (accessed 8 Aug 2012)

[12] CCP, *Online Personal Data*.

[13] Ctrl Shift, *Tracking the control shift*, Briefing Report, 2011

[14] European Commission, *Attitudes on Data Protection and Electronic Identity in the European Union*, 2011.

[15] Ofcom, *Adults Media Use and Attitudes Report*, 2012, http://tinyurl.com/czbzovo (accessed 8 Aug 2012)

[16] Ofcom, *Internet Use and Attitudes: 2012 Metrics Bulletin*, July 2012, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/2012_metrics_bulletin.pdf (accessed 8 Aug 2012)

[17] PricewaterhouseCoopers LLP, *Research into Consumer Understanding and Management of Internet Cookies and the Potential Impact of the EU Electronic Communications Framework*, commissioned by the Dept. for Culture, Media and Sport, 2011.

[18] Ofcom, *Adults Media Use and Attitudes Report*, 2012, http://tinyurl.com/czbzovo (accessed 8 Aug 2012)

[19] CCP, *Online Personal Data*.

[20] D. Boyd and E. Hargittai, 'Facebook privacy settings: who cares?', *First Monday* 15, no 8, 2010, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589 (accessed 17 Apr 2012)

C. Edwards and C. Fieschi (eds.), *UK Confidential*, London: Demos, 2008, www.demos.co.uk/publications/ukconfidential (accessed 17 Apr 2012)

European Commission, *Attitudes on Data Protection and Electronic Identity in the European Union*, pp 23 and 30

R. Henry and C. Flyn, 'Tap, tap, tapping us all up – mobile apps invade privacy', *Sunday Times*, 26 Feb 2012. This is related to the Eurobarometer data that found that 58 per cent of UK respondents read privacy statements on the internet.

[21] CCP, *Online Personal Data*.

[22] 'We need to build a much closer relationship between government, the private sector and the public when it comes to national security', Cabinet Office, A Strong Britain in an Age of Uncertainty: The National Security Strategy, Oct 2010

[23] UK Government, *Government efficiency, transparency and accountability*

https://www.gov.uk/government/topics/government-efficiency-transparency-and-accountability (accessed 12 Dec 2014)

[24] UK Government, Open Policy Making Blog, https://openpolicy.blog.gov.uk (accessed 12 Dec 2014)

[25] UK Government, *PM sets ambitious open data agenda,* July 2011,

https://www.gov.uk/government/news/pm-sets-ambitious-open-data-agenda (accessed 12 Dec

2014)

[26] Ipsos MORI, *Ipsos MORI Veracity Index*, 2011, http://www.ipsos-mori.com/Assets/Docs/Polls/Veracity2011.pdf (accessed 12 Dec 2014)

[27] Ipsos MORI, *Ipsos MORI Trust Poll*, 2013, https://www.ipsos-mori.com/Assets/Docs/Polls/Feb2013_Trust_Topline.PDF (accessed 12 Dec 2014)

[28] Metropolitan Police, *Communities Together*, http://content.met.police.uk/Site/communitiestogether (accessed 12 Dec 2014)

[29] A. Myhill, National Policy Improvement Agency, *Community Engagement in Policing*, *Lessons from the Literature*, Nov 2012, http://college.police.uk/en/docs/Community_engagement_lessons.pdf (accessed 12 Dec 2014)

[30] Home Office, *Protection of Freedoms Act* 2012, Oct 2012, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118174/magistrates-courts-eng-_wales.pdf (accessed 12 Dec 2014)

[31] J.V. Roberts and M. Hough, Ministry of Justice*, Public Opinion and the Jury: an International Literature Review,* February 2009, http://www.icpr.org.uk/media/10381/Juries%20MOJ%20report.pdf (accessed 12 Dec 2014)

[32] A. May, Interception of Communications Commissioner's Office (IOCCO), *Annual Report 2013*, Apr

2014, http://www.iocco-uk.info/sections.asp?sectionID=1&type=top (accessed 12 Dec 2014)

[33] Liberty Publishes, *Liberty Publishes Report on Policing of the TUC March for the Alternative*, Apr 2011,

https://www.liberty-human-rights.org.uk/news/press-releases/liberty-publishes-report-policing-tuc-march-alternative (accessed 12 Dec 2014)

EE

EE welcomes the opportunity to participate in your review and welcomes the wider debate and review of investigatory powers. The existing legislative framework supporting the retention and acquisition of Communications Data (CD), the provision of Lawful Interception (LI), including the safeguarding and oversight of such, has fallen behind as technology advances and is becoming less valid in the internet age. In light of Edward Snowden's revelations, and the subsequent public concerns, together with the huge and rapid advances in technology, EE believes that a wholesale review of legislation is required. Whilst the review is likely to focus heavily on legislative reforms, it is important that a number of key issues are recognised and taken into account as part of any recommendations, namely volumes of data and associated storage, the distinction between, and definitions of, CD and content and other associated terminology, technological issues, encryption and the impact of new products and services. We provide further detail and explanation to these issues below.

We would welcome the opportunity to discuss our answers with you in private or in group sessions with industry colleagues. If you would find it beneficial, we would be very happy to invite you to see the EE operation in action at our offices in Hatfield or Bristol. The Joint Parliamentary Committee charged with the review of the Communications Data Bill visited our offices in the course of their work and we understand, found the visit useful. Please note that we would like to keep the contents of this letter confidential but we would be happy to discuss further the possibility of including certain elements of our letter in your report following your review.

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.*

In many respects traditional voice and text services are being superseded by other methods of communication. Circuit switched networks are being replaced by IP based technologies, in which voice, text and data are transmitted in packets across the network (packet switched). EE provides a connection to the internet where data is sent and received by the EE customer. In framing legislation on interference with communications, government must take into account the shift away from traditional methods of communication towards the use of this packet switched technology, and also so-called 'over the top' or OTT methods of communication.

With regards to OTT services, the CD and content of these communications are wrapped up in the data flowing across the EE network and EE has no business interfering with these communications (including the collection and retention of data relating to these

[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.

communications). EE would have serious concerns if there was an obligation on communications service providers (CSPs) to collect and retain OTT data or “third party data” as referred to in the 2012 proposals because of the impact it would have on EE’s business and EE’s ability to provide competitive services as further explained in question 3. On the technical side of things, it must also be recognised that there would be clear challenges relating to the collection and storage of this third party data.

In relation to the collection of this data, EE is concerned that there would be practical difficulties in distinguishing CD from content as changes in technology have blurred the lines between what is and what is not content. In addition, if CSPs were to be directed to collect data relating to the communications of EE customers using OTT services, EE would have to extract all information (including content) in order to filter out and retain the CD relating to that communication.

In addition, it must be appreciated that any technical solutions to the gathering and/or generation of data may detrimentally affect the quality and speed of communications that CSPs can offer to their customers. CSPs could be forced to re-design their networks to meet the obligations for the collection of this data at the expense of efficiency and speed. This will have unintended consequences for CSPs where government ends up creating a two tier system where CSPs take longer to bring a service with full facility to market by comparison with others. EE would also be concerned that it could add complexity to otherwise straightforward network changes required in the normal running of a commercial CSP, for example the flexible routing of traffic or the integration of additional bandwidth and peering.

Furthermore, OTT communication capabilities are generally provided by overseas companies and there appears to be a general move towards the encryption of these communications which would add to the complexity for a CSP to collect such third party data. Any deployed solution could end up being a short-term solution as overseas providers are likely to consider increasing the protection of their customers’ communications by the use of encryption. The maintenance of such a solution would be near impossible as any technology used to collect CD and provide LI would need to be constantly monitored for changes to the nature of the communication to ensure the collection remains complete. In addition any solution would need to be updated to keep pace with the ever changing and expanding EE network. ***

The volume of data is expected to be huge which would be incredibly challenging regardless of any processing required to aid retrieval. Without knowing the volume of events that systems might be expected to process it is difficult to comment further on the amount of infrastructure that may be required. ***

All the above challenges are likely to be exacerbated as time goes by given the exponential use of and reliance on new technologies. To reduce the volumes of retained data, government must ensure legislation supports a flexible approach to CD retention allowing for the changing requirements of public authorities in terms of the types of CD required and the length of time it may be required for.

With regards the format of legislation itself, as part of EE’s Communications Data Bill (CDB) submission, we believed that it would not be practical to have one overarching piece of legislation that governs CD and LI. On further consideration, and based upon the recent legislative changes, we believe there is now an opportunity to create a clear, consolidated legal framework for the disclosure, retention and acquisition of CD and the provision and use of LI.

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?*

The distinction in existing law and that proposed in the CDB between CD and content is less valid as changes in technology blur the lines between what is and what is not content. An example of the blurring between content and CD, and the need for clarity is the question of what is and isn't content in a weblog. Even the definition of what a weblog is has yet to be agreed, let alone whether anything that appears after the first slash is necessarily content (for example, is www.bbc.co.uk/news/ content?) or indeed, could the actual website address up to the first slash be content. However, that is not to say that any new legislation should disregard this distinction completely. What doesn't change is the intrusion, relative to CD, into a person's privacy that access to the content of their communication results in (and any collateral damage). Protection of content of communication is of the utmost importance. Access must continue to only be granted for the investigation and/or prevention of the most serious of crimes, and any retention of data must be justified based upon a clear process of proportionality.

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 current subdivisions (subscriber, use, traffic) are not appropriate and perhaps never have been. EE believes that one of the first tasks that needs to be undertaken as part of the development of any new legislation is the creation of a common agreed glossary of terms and associated definitions. It's critical that terms (e.g. data acquisition, generation, content) are clearly understood by all so that any discussion and legal requirement is not clouded by misinterpretation. EE would suggest that perhaps in order to simplify and clarify this issue, subdivisions of CD are divided into 'subscriber data' and 'usage data'. 'Subscriber data' would relate to information about a subscriber's account, their payments and the products and services in relation to that account. 'Usage data' would relate to any data generated by the use of the products and services by a customer. The appropriate protection and access restrictions would then need to be put in place accordingly.

EE believes that it must be made clear that authorisation to acquire subscriber and usage data should not allow access to all communications data. Indeed, there should be different access levels to the data based upon sensitivity and intrusiveness of specific data sets, similar to RIPA e.g. local authorities should not have access to cell site data etc. In EE's view, it is likely that access to usage data would be considered more intrusive by customers than access to subscriber data.

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?*

The CDB proposed that UK CSPs capture and retain third party data from overseas service providers. However, this would be a huge challenge as discussed in question 1. In EE's view, this would add an unacceptable amount of responsibility upon UK CSPs including increased regulatory burdens, disclosure requirements and potential liability. In addition, there would be very serious concerns in terms of confidentiality of customer data and CSP's data and systems which in our view could also very much undermine confidence in UK CSPs.

*** It is therefore EE's view that further work should be done to enhance mutual legal assistance treaties to obtain communications data which is stored overseas or indeed other international instruments and law enforcement mechanisms to make them work in light of the use of global technologies and threats.

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?*

As provided in questions 1 and 4, EE sees many problems with a mandate on CSPs to extract and retain third party data relating to overseas OTT services. The answer may lie in doing more work to enhance international co-operation.

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?*

EE believes that there should be international cooperation on law enforcement issues; however, EE is well aware that they are huge complexities and vast differences between countries and different levels of international political will to implement such cooperation. We therefore think that a single international regime is unlikely to emerge soon. However, at base level, a single international regime should place similar obligations for the retention and disclosure of CD and the provision of LI regardless of where services providers are and whatever the nature of their offering. It must be future proof and flexible but specific and narrow in scope and must take account of the right to privacy and the confidentiality of communications.

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 Single Point of Contact (SPoC) system is essential to the maintenance of a tried, tested and trusted relationship between CSPs and those requesting CD and ensures that CD is only disclosed to those with the authority to ask for it. The use of automated systems for the requesting, processing and fulfilment of requests for CD from the majority of RIPA authorities ensures efficiency and the safe handling and transfer of data relating to EE customers and the oversight of the system gives us confidence that the system isn't abused and requests are only submitted after strict tests of necessity and proportionality. The same can be said for the regime in place to support the provision of LI to the intelligence agencies and again the oversight of LI assures us that the tests of necessity and proportionality are rigorously enforced and the fact that a Secretary of State must sign a warrant for interception shows the recognition of the intrusion associated with the request.

Safeguards and oversight are key and in our opinion the RIPA regime from a controls, checks and balances perspective works well. Oversight of LI and the acquisition of CD under RIPA by the Interception of Communications Commissioner's Office (IoCCO) is crucial. ***

***

In relation to the 'Request Filter', this was explained to us in 2012 as a way of limiting collateral intrusion for law enforcement to use CD in a filtered way to obtain answers to complex questions in the course of an investigation. *** However, the points that EE raised in responding to the CDB's call for evidence, remain pertinent, including that:

- EE has a responsibility to its customers to protect their information and privacy and EE would be concerned if a huge database were to be created containing customer information outside of EE's walls. Indeed, the new databases could become a target for hackers and any data breach would have devastating consequences. There will undoubtedly be a need to balance locking the data down and allowing efficient access to comply with disclosure requests and costs issues (the costs of security will potentially be extremely high). Any security breach would have a devastating reputational impact for CSPs.
- Arrangements should be in place to ensure that a 'filtering agency' is acting (in data protection terms) as data processor on behalf of the government and that the government remains at all times responsible for the filtering agency's compliance with the Data Protection Act 1998 including data security and in the case of any data security breach relating to the Filter Request, it would remain the government's responsibility and not the CSP's.
- To fully understand the impact of the filtering arrangements, EE would need to understand what kind of request it is likely to receive from the filter agency and the anticipated volume of requests.
- EE has raised concerns in relation to the evidence of data as no single party *w*ould be able to ensure the quality of data from an evidential point of view. For example, the filtering agency would not be able to give any evidence on the source data – it would only be able to give evidence in relation to its own processing.

***

***

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?*

Encryption is a key issue to address as part of the future exploitation of existing and new data. As a direct result of surveillance as perceived by citizens and companies wanting to show that they respect their customers' privacy, more and more companies are encrypting their services to protect their customers' data. Encryption is taken as a 'given' and consumers expect greater and more robust levels of encryption. In relation to OTT services, as the communications are third party data (i.e. not generated by the CSP) the CSP would therefore have no knowledge of the encryption technologies, or the regularly changing algorithms required to decrypt this data. Any use of this data would either require the CSP to simply send that entire data stream to Government in order for them to conduct their own decryption techniques on the data, or for HMG to legislate requiring these service providers to conduct decryption in specifically defined circumstances (for example, if it relates to content when a warrant is in place). This would be as previously discussed a challenge when it relates to overseas providers.

9. *What more could be done to exploit the communications data and intercept that is currently available and likely to continue to be so?*

Until all stakeholders (HMG, Industry, Law Enforcement etc.) understand the problems law enforcement is experiencing and facing and what data is required to be exploited to meet the strategic objectives, this is a difficult question to answer. The present DRIPA position (based upon the 2009 Regulations) provides law enforcement with relatively clearly defined data sets CSPs retain for business purposes. However, in the future, additional data may be generated and could be of use to law enforcement, and discloseable under RIPA. This would place obligations upon CSPs to be able to access and disclose data in a readable format and in a timely fashion. Therefore, a flexible technical approach for data retention and acquisition, enabling the assessment and introduction of new data types should be considered. Before introduction strict tests of necessity and proportionality would need to have been met and privacy, feasibility and cost implications taken into account. The challenge is to identify the types of data that would be of benefit to assist the enforcement agencies, scope out the challenges of obtaining, interpreting and understanding that data, and then scope out the associated privacy and costs impact.

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 arrangements in the UK, by which legislation allows Government to reimburse reasonable costs incurred by CSPs, are unique. *** This model must not be allowed to weaken or 'reasonable costs' reduce, and these arrangements must be included within any future primary legislation. Indeed, EE would encourage a review of the current regime to ensure that there is a level playing field with regards costs reimbursed to industry, and that these reimbursements are fair. *** EE would like to see the current model re-assessed particularly with regards to ongoing capital expenditure to maintain LI capabilities as our network changes and evolves. This becomes more critical if the lines between LI and CD are blurred and CSPs could be required to use LI systems to extract certain types of CD for retention.

In relation to the retention of data, cost reductions will only be achieved with a targeting of data types (and associated retention periods) that are of strategic benefit***. Data volumes will only continue to increase dramatically in the future, with associated costs increasing exponentially, so a strategic approach to data identification, storage and acquisition needs to be implemented. Systems need to be future proof and configurable (both with the types of data being stored within them and the length of time the data is retained), preventing significant additional costs.

11. *How should the government organise its relationship with communication service providers, both when framing legislation on interference with communications, and routinely?*

*** Industry is key to ensuring that government has a full understanding of new technologies and the associated implications of this technology on strategy and legislation and vice versa, industry needs to ensure that they can plan their own network developments, services and business strategies with the full knowledge of how these will be impacted by government policy. This requires a constant building of the partnership between industry and government at a senior level, and also at operational levels. *** The National Policing/Communications Industry Communications Data Strategy Group (CDSG) provides a forum, comprising senior members from Industry, law Enforcement and Home Office, to discuss policy, legislative and strategic matters relating to CD retention and acquisition. This group is proving beneficial and allowing key stakeholders the opportunity to debate and influence government policy. ***

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.*

The following concerns (also raised by EE as part of the CDB) are relevant:

- Although EE understands the need to maintain capability and the importance of communications data in preventing and detecting crime and saving life, any new powers could place too much of a responsibility and too much liability upon UK CSPs. There could be increased regulatory burdens beyond current legal obligations, increased demands and amounts of disclosure to third parties and additional liability risks.
- There are very serious concerns in terms of confidentiality of customer data and confidentiality of the CSP's data and systems which in our view could also very much undermine confidence in UK CSPs. As people spend more time online and make ever greater use of internet-based services, the collection and retention of communications data about their internet usage undoubtedly raise significant issues for individuals' privacy. The question is whether this level of intrusion into people's online behaviours and the interference with the confidentiality of their communications is proportionate.
- CSPs should be able to give transparency to their customers. If we are unable to be transparent about the data we are being required to gather and retain, it will appear to our customers as if we are secretly snooping on them.
- Data security is of the utmost importance for the public to trust private companies and government.
- There should be suitable penalties for public authorities' employees if they breach statutory codes of practices relating to access to and use of CD and LI.

Jonathan Grayling
Government Liaison and Disclosures

(This response includes redactions to ensure that no commercially sensitive information is disclosed.)

October 2014

Equality and Human Rights Commission

Executive Summary

1. The Equality and Human Rights Commission (the Commission) considers that the Regulation of Investigatory Powers Act 2000 (RIPA) needs significant reform.

2. Firstly, the structure of the protections in the Act is no longer fit for purpose: it establishes a series of tiers of protection based on distinctions between content data/communications data; and internal/external communications which no longer adequately reflect privacy concerns or the intrusiveness of the powers in question.

3. Secondly, in relation to targeted interception warrants there are issues around the breadth of the definition of 'national security' and the role of the Investigatory Powers Tribunal in ensuring effective oversight, though these are less serious than the issues relating to external communications and communications data.

4. Thirdly, in respect of interception of external communications, the section 8(4) regime is apparently capable of capturing a vast amount of people's every-day internet use, email and telephone activity. There are strong arguments that the regime fails to meet the minimum standards required for compliance with Article 8 of the European Convention on Human Rights (ECHR).

5. Fourthly, the regime for obtaining communications data under Chapter II of RIPA contains fewer, probably insufficient, safeguards despite the fact that communications data can in fact be as revealing and intrusive into personal privacy as content data. Clear and precise rules need to be established in order to regulate the receipt and use of communications data held by private companies in order to comply with Articles 8 and 10.

6. Finally, the current oversight arrangements have not demonstrated that they are effective in achieving accountability in relation to interception of communications and the Commission is of the view that a new regime of independent authorisation should be devised.

Introduction

7. The Commission welcomes this timely and much needed Review. Given the already fragmentary nature of RIPA identified in the Commission's 2011 research report,[1] we have long considered the legal framework governing privacy and surveillance should be the subject of general review rather than piecemeal reform.

8. The Commission has engaged in 2014 with the Intelligence and Security Committee's Inquiry into Privacy and Security both by giving evidence in writing and in person. Our submission to this Review builds on that work and our response to the ISC is attached to this document at Annex 1[2].

9. Whilst the law in this area is largely reserved, there are some limited implications for the devolved administration in Scotland which will need to be fully taken into account in any programme of legislative reform.

10. In summary, the Commission's established position on these issues is as follows:

    - Whilst details of surveillance operations must remain secret, more could be done to demonstrate to the public that surveillance decisions are made in a manner that respects fundamental rights, for example by greater openness by the Interception of Communications Commissioner.

    - It is difficult to set out in abstract terms how the right to privacy should be balanced against the right to security and the right to life, and a 'one size fits all' approach should not be adopted across the broad range of areas involving surveillance and investigatory powers.

---

1 Charles Raab and Ben Goold, *Protecting Information Privacy* (Equality and Human Rights Commission Research Report No 69; 2011) at p3.

2 We are grateful to Eric Metcalfe of Monkton Chambers for advice in relation to the ISC Inquiry and to Tom Hickman of Blackstones, for his advice in relation to the issues covered in this submission.

- Privacy considerations should depend on the type of information and in particular the degree of its private nature, and not on the type of technology at issue. For instance, internet communications vary in their level of privacy, with communications between friends on closed messaging groups differing from posting on twitter or YouTube. Furthermore, emails and skype calls have more in common with traditional mail and telephone calls than with other forms of internet communications.

- "Mass" or "untargeted" collection and monitoring of private communications raise particular concerns. Whilst such a facility might be useful to the authorities in combating crime, the test of necessity is not to be equated with being useful, reasonable, desirable or expedient, according to the long- established jurisprudence of the European Court of Human Rights ("ECtHR").

- Domestic law embodies a long-standing distinction between "communications data" (data about data; broadly speaking, the who, where, when and to whom, of a communication) and "content". However, given technological developments, communications data can disclose highly sensitive information about a person's private life, even if the actual content of the information is not disclosed.

- The mere collection of private data constitutes an interference with privacy and blanket retention in the absence of reasonable suspicion constitutes a disproportionate interference.

- The warrant regime for interception of communications under RIPA is (1) heavily dependent on internal self-authorisation, and (2) does not require targeted surveillance in respect of "external" communications, which can include all communications routed outside the British Isles. It is unclear what the scope of this power is and whether Facebook and search engine requests are internal or external communications.

- Ethnic minorities are also more likely to be impacted by external communications warrants, since a recipient is more likely to be overseas, and thus have less protection.

11. We have previously made five proposals for reform. In short, (1) consideration of the need for judicial authorisation; (2) clarification of internal/external distinction; (3) targeting for all warrants; (4) a new, single, oversight body to replace the patchwork system currently in place and (5) further reforms to the ISC.

12. Here we have not sought to address each of the issues in the Review's terms of reference. In particular the Commission has no particular remit or expertise in relation to:
    - Current and future threats, capability requirements and the challenges of current and future technologies;
    - The implications for the legal framework of the changing global nature of technology; or
    - The statistical and transparency requirements that should apply.

13. We address below the other three issues, namely:
    - The safeguards to protect privacy;
    - The case for amending or replacing the legislation; and
    - The effectiveness of current statutory oversight arrangements.

The safeguards to protect privacy

Legal requirements

14. The interception, storage and use of private information engages the protections of Article 8 ECHR

15. It is a long-established principle of the ECtHR that whilst the law cannot be set out in such detail in public that an individual can foresee when the authorities are likely to intercept his communications, nonetheless the *"law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life…."*: Malone v United Kingdom, 2 August 1984 (1985) 7 EHHR 14 at 67.

16. The ECtHR has developed the following "*minimum standards*" that should be set out in "*statute law*" as "*clear, detailed rules*", which should include:

    - the nature of the offences/conduct which may give rise to an interception;
    - a definition of the categories of people liable to have their communications intercepted;
    - a limit on the duration of interception;
    - the procedure to be followed for examining, using and storing the data obtained;
    - the precautions to be taken when communicating the data to other parties;

- the circumstances in which communications must be destroyed. See Weber v Germany (2008) 46 EHRR SE45 at 92 and 95; Liberty v United Kingdom (2009) 48 EHRR 1 at 62-63.

17. As the Court recently reaffirmed in Telegraaf Media Nederland Landelijke Media BV v The Netherlands, App. No. 39315/06, 22 Nov 2012 at 98, "[i]*n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*". In an appropriate context, and where other safeguards are sufficient, the Court has been prepared to accept that "*independent supervision*" is adequate.

18. In Klass v Germany (1979) 2 EHRR 214, the Court held that the practice of seeking prior consent for surveillance measures from the G10 Commission, an independent body chaired by a president who was qualified to hold judicial office and which had power to order immediate termination of the measure, was adequate.

Current protections for privacy

19. The main legislative provision addressing the interception of communications by public authorities and interception of communications by public authorities is RIPA.

20. The object and purpose of RIPA was to establish a regime that was compliant with Article 8 of the ECHR. The then Home Secretary Jack Staw MP stated in introducing the Bill to Parliament on 6 March 2000 that the Bill:

> "represents a significant step forward for the protection of human rights in this country. Human rights considerations have dominated its drafting. None of the law enforcement activities specified in the Bill is new. What is new is that, for the first time, the use of these techniques will be properly regulated by law and externally supervised. …. The regime set out in the Bill will ensure that the regulation is compatible with the terms of the convention." (HC Debs. 6 March 2000, Cols. 767-768).

21. He also said that law enforcement bodies would benefit from clear guidance on the precise circumstances in which they can use particular techniques and the public will benefit because, *"the circumstances in which the powers can be used will be clear to them*."

22. We are here concerned with interception of communications and use of communications data, not with the other investigatory techniques (such as use of covert sources) that RIPA regulates.

23. RIPA draws a distinction between private and public telecommunication systems. Interception of communications on private communications systems is permitted for ordinary business purposes or with express or implied consent of those effected (ss. 1(6) and 4(2)).

24. The protection regime for communications on public communication systems established by RIPA has the effect of creating several tiers of protection for receipt and use of data by public authorities derived from public telecommunications systems.

25. First, there is the **content of communications between persons in the British Isles** on postal service or public telecommunication systems. This is regulated in Chapter I of Part I of the Act. Such information can be obtained:

(1) By warrant issued by the Secretary of State; (2)On application by:

- MI5, MI6, GCHQ and Chief of Defence Intelligence;
- The National Crime Agency;
- Met Police, Police Services of Northern Ireland and Scotland;
- Competent foreign authorities for mutual assistance purposes.

(3) Where the Secretary of State believes that the warrant is necessary:

- In the interests of national security (s.5(2)(a), s.5(3)(a));
- For the purposes of preventing of detecting serious crime (s.5(2)(a), s.5(3)(b));
- For the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well— being of the United Kingdom (s.5(2)(a), s.5(3)(c); or
- For the purpose of satisfying a mutual assistance request in circumstances equivalent to those in s.5(3)(b) where the request relates to acts or intentions of persons outside the British Isles (s.5(2)(a), s.5(3)(d), s.5(5)).
- And that the conduct is proportionate to what is sought to be achieved by that conduct (s.5(2)(b)).

(4) The warrant must name or describe an interception subject or a single set of premises as the object of the interception. The warrant must set out a schedule including addresses, numbers apparatus or other factors for identifying the communications.

(5) Interception material is inadmissible in any legal proceedings (save exceptionally some relating to national security) (ss.17, 18).

26. Secondly, there is **content of communications between persons which are "external communications"**. This is also regulated by Chapter I Part I of the Act. External communications are defined as those that is sent or received outside the British Isles: RIPA s.20. In such as case, requirement (4) above does not apply. That is to say, such warrants can be non-targeted. However, the warrants can only be granted if it is believed that they are necessary for one of the purposes set out in, s.5(3)(a)-(c) (excludes formal mutual legal assistance requests) and that the examination of that material is necessary: ss.8(4)(b), and 16(1)(a).

27. Thirdly, there is the acquisition of **communications data** whether relating to internal or external communications. This is regulated by Chapter II of Part I of the Act. Such information can be obtained:

(1) On application by the intelligence services, police forces, HM Revenue and Customs and a wide range of other Departments, agencies and local authorities, fire authorities, licensing authorities (etc.) specified in the RIPA (Communications Data) Order SI 2010/480 Schedule 2.

(2) With the authorisation of a designated person holding a specified senior rank or office (s.22(3)) or by notice requiring a telecommunications company to supply the information (s.22(4)). In the case of applications by public authorities, there must also be approval from a magistrate (s.23A).

(3) Where the applicant believes it is necessary:

- In the interests of national security (s.22(2)(a));
- For the purpose of preventing or detecting crime or preventing disorder (s.22(2)(b);
- In the interests of the economic wellbeing of the UK so far as relevant to the interests of national security (s.22(2)(c));
- In the interests of public safety (s.22(2)(d) or public health (s.22(2)(e);
- For the purposes of collecting any tax, duty, levy or other imposition, contribution or charge payable to the Government (s.22(2)(f));
- For the purpose, in an emergency, of preventing death or injury or mitigating any injury (including to mental health) (s.22(2)(g); or
- To assist identification of dead or incapacitated persons and to assist investigations into miscarriages of justice (The Regulation

of Investigatory Powers (Communications Data) Order 2010.

(4) The authorisation must be in writing, must describe the conduct authorised and the communications data to be obtained, must specify the reasons why it is necessary and must specify the rank, office or position of authorising person (s.23, Coms. Code paras 3.23-48).

28. Section 15 of RIPA sets out some "general safeguards" which apply to intercepted communications. It imposes a duty on the Secretary of State to ensure that arrangements are in place for ensuring that the number of persons to whom any of the material or data is disclosed, the extent of disclosure and copying of material resulting from interception, *"is limited to the minimum that is necessary for the authorised purposes"* (s.15(2)). It also requires copies to be destroyed unless it continues to be *"or is likely to become"* necessary for one of the authorised purposes.

29. Section 16 of RIPA sets out "extra safeguards" relating to section 8(4) warrants, in cases where intercepted material is selected to be read or examined but where the individual is known to be in the British Islands and where such examination is intended to identify material sent or received by him. This material can only be examined if certified to be necessary by the Secretary of State and is limited to communications during a three month period (six months in the case of national security) (s.16(3), (3A)).

30. In respect of section 8(4) warrants, media reports suggest that the British Government has, under a programme known as TEMPORA, obtained a general warrant under s.8(4) to intercept all external communications passing between Europe and the USA (through the British Islands) and that these communications are then filtered by use of volume reduction techniques and "selectors" (a form of search term). This warrant is renewed on a rolling basis.

31. In accordance with its standard practice, the UK Government has refused to confirm or deny the TEMPORA programme and the process and conditions for filtering such data has not been disclosed even in outline. However, in a witness statement served (and made public) in current proceedings before the Investigatory Powers Tribunal ("IPT") brought by Privacy International and Liberty, Mr Charles Farr, Director General of the Office for Security and Counter Terrorism, has confirmed that, *"interception under the s.8(4) regime takes place at the level of communications cables, rather than at the level of individual communications."* (at 139).

32. Mr Farr also stated that, "*the United Kingdom's section 8(4) regime, involve[s] the interception of volumes of communications and the subsequent performance of a process of selection with respect to those communications to obtain material for*

further consideration by Government agencies." (at 150) This confirms the general nature of the interception programme and the use to which section 8(4) is put in practice.

33. Section 57 of RIPA establishes the Interception of Communications Commissioner who has statutory responsibility to review the exercise of the powers under Chapter I and Chapter II of RIPA. Section 65 establishes the IPT to hear complaints relating to interception of communications or receipt of communications data.

34. Two relevant Codes of Practice have been made under section 71 of RIPA: "Acquisition and Disclosure of Communications Data" ("Comms Code") and "Interception of Communications" ("Intercept Code").

The case for amending or replacing the legislation

The structure of the protections contained in the Act is no longer fit for purpose

35. The case for amending or replacing the legislation relates in large part to the fact that the structure of RIPA no longer adequately corresponds to the privacy concerns arising from the interception of communications and use of communications data given technological developments.

36. In particular, the structure of RIPA, as explained above, reflects the belief that interception of the content of communications of persons in the UK is the most intrusive and problematic for residents of this country and deserving of greatest protection; next important is content of external communications; whereas obtaining communications data raises far fewer issues and therefore is subject to far fewer safeguards, in particular is not subject to a warrant regime and is available to a much wider range of public authorities.

37. However the importance of these distinctions has been eroded.

38. Consider first the distinction between communications data and content data. Communications data is information about communications: about the identity of sender and recipient of the communication and the method of communication. At the time RIPA was enacted a common analogy used to describe the distinction between communications data and content data was that it was equivalent to information on the outside of an envelope and the information inside an envelope.

39. However, technological developments in the telecommunications sector have meant that there is far more communications data available about people and it is far more revealing about the movements, associations, likes and dislikes, of such persons than previously.

40. Communications data includes (a) traffic data; (b) service use data; and (c) subscriber information.

41. **Traffic data** is information about communications, excluding the content of those communications. This can include not only the origin and destination of a communication but in the modern age it enables information to be obtained about the movements of mobile devices such as cell phones and information about web browsing including, host machine, server, IP address (whether mobile or static) and websites visited (but not specific pages viewed) (s.21(4)(a), s.21(6) RIPA, Comms Code 2.19-2.22; Part 2. Part 3). (– Local authorities are not permitted to obtain traffic data.)

42. **Service use data** is information identifying the use made by a person of a telecommunications or postal service, such as itemized call records, itemised internet connections, timing and duration of services used, information about the amount of information uploaded or downloaded, records of special services used such as conference calls (s.21(4)(b), Comms. Code 2.23-2.24).

43. **Subscriber information** is about customers of telecommunications service providers, and can include itemized telephone records, identity of email account holders, identity of persons with posting access to a website, information on how accounts were paid, billing and installation addresses, any demographic information supplied to a service provider (s.21(4)(c) RIPA, Comms Code 2.25-2.29).

44. It is obvious that obtaining such information can be enormously revealing about a person, including about their friends and associates, movements, lifestyle and habits. It is widely recognised that communications data can often be more revealing about a person than content information, and certainly it potentially enables a very detailed picture to be built up about a person's private life.

45. However, such information is subject to much weaker protections than intercepted communications and is available to a far wider range of public authorities. The fact that authorisation does not have to be approved by the Secretary of State means (save in respect of local authorities which are subject to a judicial approval regime) that the authorisation is not independent of the organisation concerned (let alone, of course, independent of government) and there is an absence of direct accountability to Parliament.

46. The second distinction of importance to RIPA is between external and internal communications. Again, the global technological revolution of the internet has greatly reduced the utility of this distinction. The internet does not recognise national boundaries, many websites are hosted abroad and many internet service providers maintain servers abroad.

47. Part of the issue is the fact that a "communication" under RIPA is not limited to two persons communicating with each other, but can include a person's communication with an electronic system. It thus embraces, for instance, not only web-mail and email communications, Twitter and Facebook posts, but google searches and internet browsing (see Comms Code at 2.13, 2.120).

48. The Code of Practice on Interception of Communication prohibits (at 5.1) prohibits the characterisation of internet uses as "external communications" merely because the message is routed via a server located outside the UK. However, where the intended recipient of the message is a website that is outside the UK this is regarded as an external communication. And, it appears, this is treated as including cases in which a message is posted to a website or platform that is hosted outside the UK. Thus, Mr Farr states in his witness statement:

> "*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). …*
>
> *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 outside the British Islands. In such a case, the search would correspondingly involve two "external communications" for the purpose of section 20 of RIPA and paragraph 5.1 of the Code*." (statement dated 16 May 2014 at 133-134)

49. Since the server processing the google seach may in fact not be outside the UK, the question whether the use of a search engine or other similar internet use involves an "external communication" can be fortuitous and unrelated to the actual character of the activity in question (an internet search).

50. Mr Farr goes on to explain that YouTube postings are regarded as "external communications" as are Facebook postings and Tweets on Twitter . If any such post is made on a platform that is based outside the British Islands then they are treated as external communications.

51. The result is that any internet use that involves communicating with a website that happens to be hosted outside the British Islands will constitute an external communication. This will mean that it falls outside the protections contained in sections 8(1) and (2) of RIPA for targeting of individuals and is subject to bulk interception. This un-targeted intercept material is then subject to the un-published internal conditions on reduction and selection of material for examination.

52. This is both arbitrary (because it is arbitrary whether the website is hosted outside the UK) and does not relate to an ordinary understanding of the notion of an external or overseas communication. It also means that section 8(4) of RIPA provides a back door which enables gigantic amounts of communications to be intercepted and searched without application of the statutory protections. It is possible (although this is not known) that rather than the greater part of internet usage in the UK not being subject to interception save where a targeted warrant is obtained; in fact the greater part of internet usage in the UK is subject to automatic bulk interception and examination subject to unknown procedures.

53. Thus, there is a general problem with the RIPA regime which relates to the fact that it establishes a series of tiers of protection based on distinctions between

    - content data/communications data; and
    - internal/external communications

    which no longer adequately reflect privacy concerns or the intrusiveness of the powers in question.

Specific issues in relation to targeted interception warrants

54. In Kennedy v United Kingdom the ECtHR held that the system for targeted interception warrants satisfied the conditions set out in paragraph 8 above.

55. There are however some question marks over that judgment and it should not preclude a careful consideration of whether the regime is entirely satisfactory.

56. Firstly, the ECtHR held that the concepts of "serious crime" and "national security" were sufficiently clear to give citizens an adequate indication of the circumstances in which the power might be used (at 158-158). However, it relied upon an out-dated definition of national security provided by the Interception of Communications Commissioner in 1985.

57. Recent Court of Appeal authority has emphasised that the concept of national security is very broad, can include for example action which aids states with whom the UK has an important intelligence sharing relationship and is thus in large part a question of "foreign policy": SSHD v Rehman [2003] 1 AC 153; R (Corner House) v Director of the Serious Fraud Office [2009] 1 AC 756 CA at 139.

58. It also includes pandemics and threats to internet and communications capability and energy security, which may be used as a basis for wide-ranging and unforeseeable powers. Lord Woolf has described "national security" as a "protean concept" (ibid. at 35).

59. Furthermore, in R v Gül [2013] UKSC 64; [2013] 3 WLR 1207 the Supreme Court recently made cautionary remarks about the breadth of the definition of terrorism (which is a sub-set of national security). It held that the concept of terrorism could be applied to insurgents and freedom fighters against a government in non-international armed conflicts. It noted the very broad definition under the Terrorism Act 2000. Furthermore, the Court stated that this is "so broad" that it gives rise to "even more concerns" where it is the basis for the exercise of intrusive powers by the police or law enforcement agencies (at 63).

60. These remarks have implications for the use of the coercive powers under the RIPA because whilst the use of the powers might be within the statutory definition of terrorism, they might be used for a very wide-range of action.

61. The Independent Reviewer of Terrorism legislation has also recently stated that the definition of terrorism is too broad. Referring to the recent case involving David Miranda, he said:

> "*By holding (with faultless logic) that the politically-motivated publication of material endangering life or seriously endangering public health or safety can constitute terrorism, the court admitted the possibility that journalists, bloggers and those associated with them could, as a consequence of their*

writing, be branded asterrorists and subjected to a wide range of penal and executive constraints." The Terrorism Acts in 2013, David Anderson QC, July 2014 at 10.14.

62. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue), in a report to the UN Human Rights Council in April 2013 (A/HRC/23/40) stated that, "*Vague and unspecified notions of "national security" have become an acceptable justification for the interception of and access to communications in many countries*." (at 58) As described above, that appears to be the case in the UK.

63. Secondly, in terms of the requirement of independent authorisation or oversight, the ECtHR in Kennedy v UK put considerable emphasis on the role of the Investigatory Powers Tribunal ("IPT") (at 167). This is considered further below at paragraph 99 where it is suggested that this was to place too much emphasis on that tribunal.

64. Despite these points, the regime relating to interception of internal communications is far less problematic than that relating to external communications and communications data.

Specific weaknesses in the context of section 8(4) warrants

65. In respect of interception of external communications, there are strong arguments that the regime fails to meet the criteria set out in paragraph 10 above.

66. The section 8(4) regime is apparently capable of capturing a vast amount of people's every-day internet use, email and telephone activity. This includes activities that most people would not regard as either (1) "communications" or (2) "overseas" communications.

67. Furthermore, it is not clear from RIPA or from the Code of Practice that the regime permits bulk interception of such data.

68. Until the disclosures relating to the alleged TEMPORA regime, individuals would reasonably not have had any idea of the breadth of the activities that were engaged in under section 8(4) of RIPA. Whilst reference to the Code of Conduct would have indicated that the interception regime applied to internet activity, the TEMPORA disclosures and the information contained in Mr Farr's witness statement have been revelatory.

69. The Code of Practice provides no indication that "interception of volumes of communications" was the norm under section 8(4). Moreover, paragraph 5.2 in setting out requirements for explanations of the type of material that is to be

intercepted, requiring any unusual degree of collateral intrusion by the interception to be specified and by requiring any particular intrusion on religious, medical or journalistic confidentiality to be justified, would give the impression that it is not used as a means of intercepting all external communications going to or from the British Islands. Such requirements in the Code are effectively superfluous.

70. For these reasons, it is difficult to accept that the regime sets out sufficiently clearly or accessibly the criteria for interception of people's communications.

71. As explained above, there are some conditions attached to grant of a section 8(4) warrant, but they are not extensive. The application for a warrant must include an explanation for why the interception is considered necessary for one of the reason set out in section 5(3) (Interception Code 5.2, 5.3). But this is likely to be of a very general nature, as the following statement of Mr Farr in his statement indicates:

> "*it will be apparent that 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 is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant factors.*" (at 149).

72. The justification for a warrant under section 8(4) of RIPA to intercept bulk communications would no doubt be justified in similar terms to these.

73. The warrant must also be accompanied by a certificate issued by the Secretary of State setting out "the descriptions of intercepted material the examination of which he considers necessary" (RIPA s.8(4)(b)(i)). Such a description might however also be very general and might relate to all of the intercepted material (Code 5.6). There has been no disclosure of how this provision is interpreted and applied in practice and it is not further regulated by the Code of Practice.

74. Section 9(1) provides for the expiry of an interception warrant unless renewed. But in practice this does not impose any significant control, because general warrants are not based on any particular individuals or specific threat, but general threats to national security. As in the case of Gillan and Quinton v UK (2010) 50 EHRR 45, at 81 the alleged statutory temporal restriction has failed, so that a "rolling programme" of indefinite authorisation is effectively in place.

75. The Code requires that a person applying for a warrant must supply a general assurance that they will comply with the "general safeguards" contained in section 15 RIPA and the "extra safeguards" contained in section 16 (Intercept Code 5.2). But both sets of protection are of limited scope.

76. They require the Secretary of State to ensure that arrangements are in place to secure that the number of persons to whom intercepted material is disclosed and the extent of copying is "limited to the minimum that is necessary for the authorised purposes": section 15(1), (2). The material must be destroyed if there are no longer grounds for retaining it for "authorised purposes": s.15(3) However, "authorised purposes" are extremely wide (s.15(4)) and include where the information is or "is likely to become" necessary for any of the purposes specified in s.5(3).

77. Thus, information can be used for any purpose relating to national security, preventing or detecting serious crime (etc) and can be kept even if it is not of any current utility. Moreover, it does not require the continuing or future utility of the information to be connected to the particular basis on which it was obtained, but can be retained so long as it is thought likely to be of any future utility to national security in general. There is also no requirement, in RIPA or the Code, which stipulates when the material should be reviewed (the Code refers to review "*at appropriate intervals*" at 6.8).

78. This relatively relaxed regime for the retention of data is easier to justify in the context of internal interception warrants because the individual concerned will have been a specific target of law enforcement bodies or the security services, but its application to persons whose communications have been obtained under a section 8(4) warrant is much harder to justify. Arguably, there should be much tighter controls where intercept material derives from bulk-collection and an unknown filtering process.

79. It is partly in recognition of the need for extra protections after the interception in the case of section 8(4) warrants that there are "extra safeguards" contained in section 16. But these are limited in scope to protecting persons who are within the British Isles who are an intelligence target by limiting the reach of a section 8(4) warrant with respect to such persons. Section 16 is intended to ensure that material obtained under a section 8(4) warrant is not examined if it is material that could be obtained by obtaining a section 8(1) warrant (i.e. it is material relating to an individual in the British Isles).
However, section 16:

(1) Permits the examination of material targeted at a person in the British Isles for periods of 3 months or six months (in the case of national security). It thus effectively allows targeting of persons in the British Isles by means of

examination of bulk data collection, and permits that for considerable periods before the authorities are required to obtain an ordinary interception warrant.

(2) Imposes no restrictions on the interception or examination of data that has been sent by a person in the British Isles where the examination is not targeted at that person – the communications of persons who are communicating with the target from within the British Isles, for instance, can be freely examined so long as this falls within the general umbrella of being in the interests of national security or combatting serious crime (etc.).

(3) Imposes no restrictions on the examination of personal data of persons not present in the British Isles, whether they are British citizens or citizens of other states, including where the selection of data is targeted at them.

80. For these reasons there are credible and powerful arguments that the regime relating to section 8(4) warrants does not satisfy Article 8. There is no effective limit on the interception set out in law and the law does not set out the procedure to be followed for examining the communications or the precautions to be taken when supplying them to third parties, such as the US National Security Agency. The regime can even be used to target individuals in the British Isles, with minimal restrictions. And the circumstances in which the communications must be destroyed, whilst specified, are potentially so broad as to effectively permit the retention of enormous amounts of intercepted information.

Weaknesses in relation to communications data

81. The regime for obtaining communications data under Chapter II of RIPA sits apart from the warrant regime. This is despite the fact that communications data can in fact be as revealing and intrusive into personal privacy as content data.

82. The principal restrictions set out in the Code relate to the time period for which requests may be made and record keeping. As to time-periods, the Code states that a particular period should be specified and where this relates to a future period the notice or authorisation should be limited to one month. This is however subject to renewal on one month intervals (Comms Code 3.43—3.46). The Code requires that:

> "*Designated persons should give particular consideration to any periods of days or shorter periods of time for which they may approve for the acquisition or disclosure of historic or future data. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the authorisation or notice and impose unnecessary*

burden upon a CSP given such notice."

83. The only substantive criterion on the obtaining of such data is that it is necessary for one of the various purposes set out in section 22(2) of RIPA. These purposes are very broad, including for example tackling "crime" and in the interests of "national security", as set out above.

84. The Code provides that data acquired and any copied data must be stored "securely" and that the data protection principles under the Data Protection Act 1998 must be complied with (Comms Code 7.1). However, the Data Protection Act exempts authorities from the data protection principles in the case of national security (s.28). Data held for the purpose of prevention or detection of crime or assessment and collection of tax is exempt from the first data protection principle – that it be processed fairly and lawfully (s.29).

85. Subject to these exceptions, the effect of these provisions is effectively to require no more by way of protection of information than is ordinarily required under the Data Protection Act.

86. It may be possible to justify this approach by reference to the fact that the information is information which is generated by companies in the ordinary course of their activities and may well be information which they would ordinarily keep for considerable periods of time under the Data Protection Act. Therefore, it could be argued, individuals have no expectation that the privacy of this information would be protected beyond the requirements of the Data Protection Act.

87. However, the obtaining of such data by public authorities differs in at least two significant ways from the obtaining of the information by private companies. Firstly, because such authorities are able to aggregate such data to build up a far more revealing picture of the activities of individuals. Secondly, because such authorities are entitled to use such information for different purposes, particularly for investigating crime and in the interests of national security, but also for a wide range of other purposes.

88. Two particular controls placed on the use of such information by the Data Protection Act are worth highlighting:

    (1) First, all information obtained, other than that obtained for national security purposes which is exempt from the data protection principles, must not be kept for longer than is necessary for that purpose (the fifth data protection principle). However, there is no time limit and no further restriction.

    (2) Data cannot be supplied to overseas authorities unless it is thought that

the territory can adequately secure the material (the eighth data protection principle). However, the Code indicates that this should not be taken as an

absolute requirement. The authority must usually be satisfied that he information will be "*adequately protected*" outside the UK, with a presumption that EU countries will adequately protect such data, but this is not an invariable requirement (Comms Code, 7.18-7.21). But the overriding principle is that the material can be transferred when it is "*in the public interest to do so"* and does not breach the Human Rights Act 1998 (Comms Code 7.12, 7.16).

89. The wide-ranging scope of the powers under RIPA for obtaining communications data were highlighted by a report in the Times on 1 October 2014 ("Police used secret phone records of reporter's source") which stated that:

> *"Police investigating the Chris Huhne speeding points scandal secretly obtained the phone records of a journalist and one of his sources for the story, even though a judge had agreed that the source could remain confidential, The Times can reveal. A Kent police officer was granted authorisation to obtain the billing and call data of a Mail on Sunday journalist, alongside his source, who was later unmasked as a freelance journalist. The pair, whose data was obtained from their landline and mobile phone service providers, …."*

90. This raises an issue under Article 10 in relation to confidentiality of journalists sources, and access to and retention of legally privileged communications. The lack of safeguards in the Chapter II regime means that there is no restriction on how material is collected, and no guidance in place to ensure that the powers are not used in a discriminatory fashion - for instance by targeting particular groups.

91. Thus, tested against the principles identified by the ECtHR as important, the current regime probably contains insufficient safeguards both as regards Article 8 and Article 10:

- There is no clearly defined set of circumstances in which the powers can be resorted to. The notions of “crime” and “national security” are especially broad.

- Independent judicial approval is lacking other than in relation to local authorities.

- There is no limit on the duration of such measures, as authorisations and notices can be renewed.

- There is no specified procedure for examining and using the information obtained. There are no safeguards for particular types of material beyond those contained in the Data Protection Act, such as in relation to journalistic material or legally privileged material.

- The restrictions on provision to third parties including overseas organisations are vague and general; as are the requirements for destruction of the information.

- There is a particular lack of structured safeguards in the context of national security information given the exclusion of the data protection principles.

92. The recent decision of the CJEU in Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Joined Cases C-293/12, C-594/12 underscores these concerns. That case concerned the compatibility of the Data Retention Directive, 2006/24/EC with Article 8. That Directive had the purpose of requiring public authorities to retain communications data for at least six months (and up to 24 months). It should however be appreciated that many telecommunications and other companies will retain data for their own business purposes and so the effect of this requirement may be quite localized in relation to particular companies or types of companies.

93. The CJEU held that the Directive contained insufficient safeguards. In doing so, it appears to have failed to appreciate that most companies will retain some or all of their data for long periods irrespective of the Directive, but its concerns about such practices indicates that greater safeguards are warranted where the retention is done by or at the behest of the government. Thus it stated:

- There was no exception for information subject to professional secrecy (at 58);

- There was no restriction on the data required to be retained by reference to particular criminal investigations or even by geography or time period (at 59);

- There were no limits on the access to the data by national authorities for purposes of prevention or protection of crime, or on their subsequent use of the data (at 60-61). The Court suggested that there must be (1) a requirement that the use of the data is "strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto" (at 61); including in respect of (2) "the number of persons authorised to access and subsequently use the data" (at 62).

- The requirement to detain for six months (with possible extension to two years) was not based on objective criteria relating to that which is strictly necessary (at 63-64).

94. The judgment in Digital Rights Ireland suggests that clear and precise rules – beyond the provisions of the Data Protection Act – need to be established in order to regulate the receipt and use of communications data held by private companies in order to comply with Article 8.

The effectiveness of current statutory oversight arrangements

95. The Commission is concerned at the low success rate of complaints before the Investigatory Powers Tribunal, which may suggest problems with the lack of transparency concerning its procedures.

96. This is an issue which was subject to an important development in the Digital Rights Ireland case because the CJEU in that case also held that of all the flaws in the regime,

> "*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*." (at 62)

97. This contrasts with the approach of the ECtHR in Kennedy v UK in which it gave the green light to the targeted warrant regime under RIPA despite the absence of any procedure for judicial or quasi- judicial authorisation.

98. In Kennedy, the ECtHR had placed considerable emphasis on the IPT. It stated:

> "*the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications.*
> *The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid.*"

99. The principal difficulty with this reasoning is that it fails to appreciate the significance of the fact that the jurisdiction of the IPT is triggered only by an individual application. Since surveillance is covert it is unlikely that any individual will make a complaint about it to the IPT (indeed, most applications to the IPT are very likely the result of paranoia where no actual surveillance has been taking place). The IPT therefore cannot sensibly be regarded as a substitute for judicial authorisation of interception of communications. It is not clear that the ECtHR fully took this into account.

100. The Digital Rights Ireland case in any event suggests that, as far as the CJEU is concerned, either judicial authorisation is required or at least a system of independent approval perhaps with judicial authorisation in the most sensitive cases. The ECtHR may in futre follow this lead.

101. Certainly, in relation to Chapter II powers, the absence even of a warrant regime raises questions about its compatibility with Article 8. The data protection regime falls under EU law and in the light of Digital Rights Ireland, the system of authorisations – even in the absence of any evidence of abuse – requires review and may require revision.

102. In respect of Chapter I powers, Digital Rights Ireland also suggests that quasi-judicial or judicial authorisation may be necessary, at least in the most sensitive cases.

103. The role of the Interception of Communications Commissioner is supervisory and he has no powers to prohibit or quash an interception warrant. He examines, *ex post*, warrants on a random basis.

104. Whilst the Commissioner fulfills a valuable 'watchdog' role, he cannot be said to compensate for the absence of judicial or independent authorisation of extremely intrusive interception warrants, particularly in the context of external communications that are subject to minimal statutory conditions and limitations.

105. Indeed, the failure of the Commissioner to highlight any concerns about the TEMPORA regime perhaps illustrates the limitations of the role.

106. The function of the ISC is more limited still (although it is democratically accountable). Pursuant to section 2(1) of the Justice and Security Act 2013, the ISC has limited authority to examine ongoing operational matters. Following the media reports following from the disclosures by Edward Snowden, the ISC issued a report (in July 2013) relating to the issue of the involvement of GCHQ with the US National Security Agency's interception programmes. However, it did not appear to have been aware of the TEMPORA programme and it did not raise any issues about it.

107. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/23/40), noted the lack of judicial oversight in the UK (at 54) and, what he described as, the attendant risk of "*de facto … arbitrary approval of law enforcement requests*" (at 56).

108. For these reasons, the Commission is of the view that a new regime of independent authorisation should be devised.

About the Equality and Human Rights Commission

The Commission is a non-departmental statutory public body established under the Equality Act 2006. It is the National Human Rights Institution for England and Wales and for Scotland for matters not devolved to the Scottish Parliament (as recognised by the United Nations under the Paris Principles, UN Resolution 48/134).

The Commission aims to work towards the elimination of unlawful discrimination, to promote equality of opportunity and to protect and promote human rights. The Commission believes that equality and human rights are for everyone and that fairness, dignity and respect are values we all share. Our role is to promote and enforce the laws that protect our rights to fairness, dignity and respect.

October 2014
Clare Collier

Annex 1

Response of the Equality and Human Rights Commission to the Consultation:

Consultation details:

Title:	Privacy and Security Inquiry – Call for Evidence
Source of consultation:	Intelligence and Security Committee of Parliament
Date:	7 February 2014

For more information please contact:

Name of EHRC contact providing response and their office address:	
Clare Collier, Senior Lawyer, Fleetbank House, 2-6 Salisbury Square, London, EC4Y 8JX	
Telephone number:	020 7832 7800
Mobile number:	07968 377824
Email address:	clare.collier@equalityhumanrights.com

Executive Summary

1. The Equality and Human Rights Commission (the Commission) considers that legislative reform is needed on this issue. We consider that an approach to determining when intrusive surveillance should be permitted based on 'balancing' potentially conflicting rights lacks clarity and rigour. Instead it could be helpful to establish a framework of principles which should govern authorisations, including the established principles of necessity and proportionality; and also legitimacy and fairness.

2. While lawful surveillance will sometimes involve interference with the private communications of individuals other than a suspect, the principle of proportionality requires that any collateral interference with others' privacy be as little as is required to assure rights to security and other human rights. We also consider that reforms of the oversight mechanisms could improve the quality and independence of the audit process, which could increase public confidence.

3. Given the already fragmentary nature of RIPA identified in the Commission's 2011 research report,[3] we consider the legal framework governing privacy and surveillance should be the subject of general review rather than piecemeal reform. We have set out at paragraph 28 some specific recommendations both to authorisation of intrusive surveillance and to oversight and accountability processes.

Introduction

4. The Commission welcomes the Committee's inquiry into this important issue. Over recent years the Commission has been involved in relevant research, litigation and briefings. We recently hosted a seminar with invited academic and legal experts to consider the questions posed by the Committee. This response

[3] Charles Raab and Ben Goold, *Protecting Information Privacy* (Equality and Human Rights Commission Research Report No 69; 2011) at p3.

is informed by that range of work, and by our legal analysis of the requirements under the European Convention on Human Rights.

5. Following recent reports concerning mass surveillance programmes by US and UK intelligence services, it is timely to review the legal framework governing access to and interception of private communications in order to ensure that the public interest in privacy and security and individual rights to privacy and security are each properly protected. As we have previously argued, the existing UK law governing the privacy of communications and information privacy more generally is in need of reform. We hope therefore that the Committee's inquiry will provide impetus for such reform.

Questions

What balance should be struck between the individual right to privacy and the collective right to security?

6. From a human rights perspective, a straightforward juxtaposition of privacy as an individual right and security as a collective one is problematic. The right of each person to be secure from threats to their person is as much an individual right as their right to privacy. The right to life under Article 2 gives rise to a positive obligation on governments to "put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life".[4]

7. All human rights are grounded not only in the private interests of individuals but also in the public interest in having those rights protected.[5] Therefore, we place social value on the right to privacy as well as the right to security.[6]

---

[4] *Öneryildiz v Turkey* (2005) 41 EHRR 20 at para 89. Grand Chamber.

[5] See e.g. Joseph Raz, *The Morality of Freedom* (1986).

[6] *House of Lords Constitution Committee, Surveillance: Citizens and the State* (HL 18, February 2009), para 102,: "the widespread use of surveillance may undermine privacy as a public good". See also e.g. JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011) at p20.

8. In this context the Commission also considers that the concept of 'balancing' these rights at the level of general principle should be treated with caution.[7] Rights protect fundamental interests and these interests do not lend themselves to being quantitively weighed in a theoretical way. These two rights are part of a framework of rights, many of which may need to be adjusted to take the others into account. Moreover, the values of privacy and security are to some extent mutually constitutive of one another: a person's enjoyment of privacy depends on that same person enjoying a degree of security against intrusion (from security measures like a lock on a door to legislation against phone hacking). Enjoyment of security can be dependant on having privacy (from personal details being divulged to a violent ex-partner, for example).

9. Respect for the right to privacy plays an important role in maintaining national security. As the former president of the UK Supreme Court, Lord Phillips of Worth-Matravers, said in 2010:[8]

> "The so called 'war against terrorism' is not so much a military as an ideological battle. Respect for human rights is a key weapon in that ideological battle. Since the Second World War we in Britain have welcomed ... millions of immigrants from all corners of the globe, many of them refugees from countries where human rights were not respected. It is essential that they and their children and grandchildren should be confident that their adopted country treats them without discrimination and with due respect for their human rights. If they feel that they are not being fairly treated, their consequent resentment will inevitably result in the growth of those who ... are prepared to support terrorists who are bent on destroying our society. The Human Rights Act is not merely their safeguard. It is a vital part of the foundation of our fight against terrorism."

---

[7] See e.g. *Protecting Information Privacy* n.1 above at p15: "Is it correct to talk about the need for a balance between privacy and the public interest, or does this suggest a false opposition between these two values?"; Jeremy Waldron, "Security and Liberty: The Image of Balance", 11 *Journal of Political Philosophy* (June 2003) 191- 210; and David Luban, 'Eight Fallacies About Liberty and Security' in *Human Rights and the War on Terror,* p243: "The supposed 'trade-off' between security and rights is too easy as long as it's a trade-off of your rights for my security."

[8] Lord Phillips of Worth-Matravers, "The Challenges of the Supreme Court", Gresham Lecture, 8 June 2010, pp 37-38.

10. Thus, an approach to determining when intrusive surveillance should be permitted by 'balancing' potentially conflicting rights would not be feasible. Instead it could be helpful to establish a framework of principles which should govern such decisions including not only the established principles of necessity and proportionality; but also legitimacy and fairness. Legitimacy and fairness bring into play important considerations relevant to public trust in the system. While it is necessary for details of surveillance operations to remain secret in order to ensure the effectiveness of those operations, more could be done to demonstrate to the public that surveillance decisions are made in a manner that respects fundamental rights. For example, although the Interception of Communications Commissioner is able to review interception warrants made by ministers, he does not review them all and the proportion of warrants he actually reviews in any given year has never been made public.[9]

11. In the individual case, there are long-established principles developed by the courts and applied by public decision-makers for resolving apparent conflicts between different rights. The right to privacy under Article 8 is a qualified right, and therefore open to governmental interference for the sake of legitimate aims such as national security and public safety where necessary. 'Necessity' is qualified both by the values of 'a democratic society', requiring governments to demonstrate a 'pressing social need' for limiting the right,[10] as well as the

---

[9] See e.g. the 2012 Annual Report of the Interception of Communications Commissioner (HC 571, July 2013) at p 14, where the Commissioner refers to "the total pool of warrants from which I select my samples for review during inspection visits".

[10] See e.g. the judgment of the Grand Chamber in *S and Marper v United Kingdom* (2009) 48 EHRR 50 at para 101: "An interference will be considered 'necessary in a democratic society' for a legitimate aim if it answers a 'pressing social need' and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are 'relevant and sufficient'".

concept of proportionality, which requires there to be "a reasonable relationship" between "the means and the aim sought to be realised".[11]

12. Security in this context refers not only to the right arising under Article 5 ("Everyone has the right to liberty and security of person.…") but also the right to life, especially to the State's positive obligation to preserve the lives of its citizens. The connection is most evident in Article 3 of the Universal Declaration on Human Rights where the concepts are grouped together: "Everyone has the right to life, liberty and security of person".

13. Although the right to life under Article 2 is framed as an absolute right, an appeal to the use of national security measures to preserve life cannot be treated as a 'trump' over other Convention rights: "not every claimed risk to life can entail for the authorities a Convention requirement to take operational measures to prevent that risk from materialising".[12]

14. It is therefore difficult to set out in abstract terms how these rights should be 'balanced'. A more specific and contextual approach is needed, but this should be founded on clear principles and be capable of taking account of the variety of contexts. . The current legal framework governing access to private communications extends across a wide range of uses, from the interception of the content of communications by police and the intelligence services under Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA), access to communications data by a broader range of public bodies under RIPA Part 2, and the more general framework governing informational privacy provided by data protection legislation, e.g. the collection of a customer's communications data by a telecom operator or internet service provider. A research paper on information privacy published

---

[11] See e.g. *Ashingdane v United* Kingdom (1985) 7 EHRR 528 at para 57.

[12] *Osman v United Kingdom* (2000) 29 EHRR 245 at para 166. Just as important, was "the need to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice, including the guarantees contained in Articles 5 and 8 of the Convention".

by the Commission in 2011 warned against attempting to seek a 'one size fits all' approach to questions of privacy.[13]

How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras?

15. It is important to be clear about the scope of the term 'internet communications'. It encompasses very different types of communication, from a text or email message sent from one person to another (analogous to a private letter sent by post), communications between a group of persons who have an expectation of privacy in their shared communications (e.g. a group of friends posting to a private mailing list or forum), communications on social media platforms (whose content may range from highly personal to extremely public, depending on the privacy settings selected), to posting on Twitter or YouTube (which may be tantamount to publishing or broadcasting to the world at large).

16. Each form of internet communication should be considered in its own right, rather than by reference to the particular technology used. For example, a Skype call is more analogous to a telephone call than to an email message (which is, in turn, closer in character to post than to Skype). There are greater similarities between a newspaper article and a news story on the BBC website than between the latter and a private message sent via Facebook, notwithstanding that the second two are both forms of 'internet communications' while the first is not.

17. The Commission would also urge against drawing any straightforward analogy between lawful surveillance of internet communications and that derived from surveillance cameras (also known as CCTV, though often no longer operated within ‘closed circuits’). Although surveillance cameras are increasingly used in a wide range of settings, including shops and restaurants, in the majority of cases they are directed at public places and therefore

[13] *Protecting information privacy,* n.1 above, at p73.

involve different expectations of privacy than would surveillance of private spaces such as a person's home. .Non-recording CCTV in a public place will not infringe Article 8[14]. A similar distinction can be drawn between communications data and content as discussed below.

18. Article 8 categorically provides that every person has a right to respect for his or her private and family life, *including* his or her 'correspondence'.[15] The Court has reiterated that protection for the privacy of a person's correspondence is not limited to letters but extends to phone calls,[16] emails[17] and general personal 'Internet usage'.[18] Whilst changes in communications technology give rise to technical challenges to law enforcement and intelligence services, they do not alter the principles governing the necessity and proportionality of lawful surveillance.

To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security?

19. Any interference in the right to privacy must be in accordance with the law, necessary in a democratic society and proportionate. Although RIPA does not itself use the term 'reasonable suspicion', the European Court of Human Rights

---

[14] *Peck v United Kingdom* (2003) 36 EHRR 41 at para 59: "monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not ... give rise to an interference with the individual's private life". However, the Court also noted that "the recording of the data and the systematic or permanent nature of the record may give rise to such considerations" (ibid).

[15] See also e.g. Article 12 of the Universal Declaration of Human Rights: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"; and Article 17(1) of the International Covenant on Civil and Political Rights: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".

[16] See e.g. *Klass v Germany* (1978) 2 EHRR 214, para 41.

[17] See e.g. *Taylor–Sabori v United Kingdom* (2003) 36 EHRR 17.

[18] See e.g. *Copland v United Kingdom* (App no. 62617/00, 3 April 2007).

has made clear that intrusive powers engaging an individual's right to privacy are unlikely to meet the requirements of Article 8 in the absence of any requirement by the authorities to demonstrate a 'reasonable suspicion' that the individual is engaged in criminal activity.[19] However, lawful surveillance will at times involve interference with the private communications of individuals other than those of a suspect, e.g. those who live and work with the subject of surveillance. Thus it is likely that lawfully targeted surveillance will result in some degree of collateral interference with the communications of persons who are not themselves suspected of involvement in criminal or terrorist activity. Such interference is 'necessary' in the sense that it is unavoidable. At the same time, the principle of proportionality requires that any collateral interference with the privacy of others be as little as is required to assure rights to security and other human rights.[20]

20. Distinguished from surveillance of an individual under suspicion is the so-called 'mass' (i.e. untargeted) collection and monitoring of private communications of the general public on a routine basis for the purpose of data-mining. Undoubtedly this may at times provide useful intelligence about the activities of a small number of suspects within the larger category. However, the legal threshold that a particular measure be "necessary in a democratic society" does not mean merely 'useful', 'reasonable', 'desirable' or 'expedient'.[21] The legislative means adopted to justify a restriction on a fundamental right on the ground of a pressing social need must be no greater than necessary.[22] Unlike the concept of 'reasonable suspicion', which may sometimes extend to a large number of individuals but nonetheless requires some evidential foundation in

---

[19] *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45 at para 86: " In particular, in the absence of any obligation on the part of the officer to show a reasonable suspicion, it is likely to be difficult if not impossible to prove that the power was improperly exercised."

[20] See e.g. section 15 of RIPA which requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorised purpose also e.g. the Home Office Code of Practice on the Interception of Communications issued pursuant to section 71 RIPA, para 6.2.

[21] *Sunday Times v United Kingdom (No 2)* (1979-1980) 2 EHRR 245 at para 59.

[22] *R v Shayler* [2002] UKHL 11 per Lord Hope, at para 59

order to be justified, the mass collection of private communications and related data deliberately eschews any form of targeting or selection. It may be possible, for example, for the authorities to have reasonable suspicion in relation to all the residents of a particular building when conducting a surveillance operation but it would be unlikely for the authorities to have reasonable suspicion against all the residents of an entire neighbourhood or city.

How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?

21. There is a long-standing distinction between communications data and the content of communications.[23] In *Malone v United Kingdom* the Court established, firstly, that the collection and use of data from private communications was not as intrusive as the interception and inspection of the content of those communications.[24] Secondly, any collection and use of communications data was nonetheless an interference with the right to privacy and therefore had to be shown to be in accordance with law, necessary and proportionate. In 2010, the Court distinguished between the collection of GPS data and other forms of video and audio surveillance on the basis that the latter "disclose more information on a person's conduct, opinions or feelings".[25]

---

[23] The terms are used here as they are used in the UK and in the human rights jurisprudence of the European Court of Human Rights.

[24] (1984) 7 EHRR 14 at para 84: "By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8."

[25] *Uzun v Germany* (35623/05, 2 September 2010) at para 52.

22. An unprecedented growth in the volume, detail and quality of 'communications data' has occurred in the past 30 yearsThe definition of 'communications data' under section 21(4) of RIPA now encompasses not just the telephone numbers dialled, and the length of the calls, but also the GPS location data (where the phone call was made or the IP address of the computer that the email was sent from), as well as subscriber data (including the credit card details held by the relevant phone company or ISP).Communications data of a person's internet use (e.g. the names of websites visited and time spent on each site) can disclose highly sensitive information about a person's private life, even if the actual content of the internet usage remains undisclosed.

23. The 'mere' collection of private data about a person is itself an interference with that person's privacy, whether or not subsequently accessed or used.[26] The Grand Chamber held that the blanket retention of DNA samples of innocent individuals once the culprit had been identified was a "disproportionate interference" with their private lives contrary to Article 8.[27] Central to the Court's reasoning was the absence of any suspicion by the authorities against the individuals that was sufficient to justify the retention of their DNA data. In a different case involving the use of stop and search powers by police under section 44 of the Terrorism Act, the Grand Chamber similarly found that the search powers did not comply with Article 8 because of the absence of any requirement on police officers to have 'reasonable suspicion' against the person subject to the search.[28] Although the police or intelligence services may have reasonable suspicions against a number of individuals in respect of the same activity, and this may justify casting a wider net when using surveillance powers, there must nonetheless be some evidential basis to justify the use of surveillance, whether or not that evidence is sufficient to identify a

---

26 *S and Marper v United Kingdom* (2009) 48 EHRR 50 at para 121: "the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data".

27 Ibid, para 125.

28 *Gillan and Quinton v United Kingdom* (2010) 50 EHRR 45 at para 86.

specific individual, rather than just because it may be useful to the authorities.

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.

24. The Commission considers that some improvements to the legal framework are required. Our report on information privacy assessed RIPA as being "marred by ambiguity, leaving open the possibility of serious errors, inadvertent use of illegal surveillance techniques, and inappropriate use of surveillance powers".[29] Among the problems identified was that access to communications data under RIPA relied heavily on "internal self-authorisation, without the requirement for judicial oversight".[30]

25. Deficiencies in the framework for authorising the interception of communications under Part 1 of RIPA mean that internet communications may be subject to two different interception regimes depending on how they are routed: communications 'internal' to the UK under section 5 RIPA and communications 'external' to the UK under section 8(4). Unlike the 'internal regime' under section 5, there is no requirement for an interception warrant under section 8 to specify that it is targeting a particular individual or premises, meaning that it can encompass broad categories of communications. Section 20 of RIPA defines 'external communications' as a communication 'sent or received outside the British Islands', but this leaves uncertainty about whether internet communications - which routinely involve contact with servers in the US and elsewhere - would be classified as 'external' or 'internal'.

26. When RIPA was debated, the Home Office gave an assurance that communications merely routed through another country would not be

---

29 *Protecting information privacy,* n1 above, at (v).

30 Ibid, p2.

regarded as 'external' communications,[31] and this is supported by the Home Office statutory Code of Practice on the Interception of Communications.[32] However, with the increasingly complex nature of internet communications, it is no longer clear whether such activities as a message posted on Facebook or a search engine request (which involve connection to US-based servers) would constitute an 'internal' communication or an 'external' one.

27. The lower threshold for 'external' communications could impact disproportionately on the privacy of members of those ethnic minorities who are more likely to have relatives overseas and therefore more likely to have their private communications caught by a mass interception warrant issued under section 8(4) RIPA.

Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications

28. Given the already fragmentary nature of RIPA identified in the Commission's 2011 research report,[33] we consider that the legal framework governing privacy and surveillance should be the subject of general review rather than of piecemeal reform. In the context of interception of communications and access to communications data, we recommend the following measures:

    (a) *Authorisation*: serious consideration should be given to introducing a requirement for judicial authorisation for interception warrants under Part 1 of RIPA. Judicial authorisation for such warrants is established practice in the Australia, Canada, South Africa, France, Germany and the

---

[31] Hansard, HL Debates, Home Office Minister Lord Bassam of Brighton, 19 June 2000: Column 104: "That does not mean that a communication sent and received inside the British Islands may be deemed to be external simply because it takes an international route."

[32] Home Office Code of Practice on the Interception of Communications issued pursuant to section 71 RIPA, para 5.1.

[33] *Protecting information privacy,* n1 above, at p3.

US.[34] Moreover, UK judges already have experience of granting similar applications in relation to asset-freezing in terrorism cases, TPIMs, and (in their capacity as Surveillance Commissioners) in approving authorisations for police to use intrusive surveillance under Part 2 of RIPA. Such a move would ensure effective independent scrutiny of the merits of any governmental request to intercept private communications, and provide evidence that any interference with the privacy rights of affected individuals was necessary and proportionate. In relation to requests to access communications data under Part 2 of RIPA, further consideration should be given to whether requests to access traffic and service use data (but not subscriber data) could meaningfully be subjected to judicial scrutiny.

(b) *Legal certainty*: due to changes in communications technology since 2000, Part 1 of RIPA no longer provides sufficient certainty to members of the public as to when their internet- based communications are liable to be subject to 'internal' interception warrants under section 5 RIPA or 'external' warrants under section 8(4). Parliament should clarify the definition of 'communication' under Part 1 as a matter of urgency.

(c) *Non-discrimination*: the existing scheme of internal and external warrants under Part 1 of RIPA, under which no targeting is required in respect of communications with persons outside the UK, could disproportionately impact on members of some ethnic minorities. It has never been suggested that the requirement for all warrants for the interception of communications internal to the UK to be targeted at either a specific individual or specific premises has prevented the effective use of lawful interception of private communications within the UK.

(d) *Oversight*: the current patchwork system of oversight commissioners under RIPA and related statutes, with seven

[34] JUSTICE, *Freedom From Suspicion: Surveillance Reform for a Digital Age* (October 2011), p 162.

separate Commissioners for the Interception of Communications, Intelligence Services, Surveillance, Information, Biometrics, and Surveillance Cameras. is fragmented, poorly resourced and unsatisfactory. There is a lack of transparency as to the degree of scrutiny provided by the Interception Commissioner, particularly given the number of warrants and authorisations that he is responsible for reviewing annually when measured against the number that he has the resources to review. We recommend the creation of a new, public-facing oversight body, to provide high quality and independent review and audit of surveillance decisions made under RIPA or subsequent legislation and with strong powers to address any unlawful or disproportionate authorisations.

(e) *Accountability*: although we welcome the grant of new powers to the Committee under Part 1 of the Justice and Security Act 2013, further reforms should be considered. As we said during the passage of the Justice and Security Bill[35], appointments to the Committee should be made by both Houses of Parliament and should not be subject to nomination or effective pre-approval by the Prime Minister. The ISC should consult and consider seriously the Prime Minister's and other views as to sensitivity of information, and should be able to redact parts of its reports. However, to ensure the required independence and effectiveness of the role, the contents of reports should be a matter for the ISC, and not subject to effective Prime Ministerial veto or censorship. We are also concerned at the low success rate of complaints before the Investigatory Powers Tribunal, which may suggest problems with the lack of transparency concerning its procedures.

[35] The briefing can be found at http://www.equalityhumanrights.com/legal-and- policy/parliamentary-briefings/justice-security-bill-with-advice/.

The Regulation of Investigatory Powers Act (RIPA) has been in place since the year 2000 and in this time the environment within which UK agencies operate has changed significantly. That environment is global in scale, but still governed by national rules of law and jurisdiction. RIPA has been amended and broadened by the Data Retention and Investigatory Powers Act 2014 in an attempt to expand the reach of surveillance authorities of UK agencies, without a comprehensive review prior to its passage. We therefore very much welcome this review and its goal to update the regulatory framework within which law enforcement and intelligence powers should be exercised. It is a rare opportunity to reflect on how UK policy should develop going forward.

Our companies take very seriously the challenges around investigating and detecting crime, and safeguarding national security. We appreciate that law enforcement agencies around the world need a timely and efficient way to collect evidence in legitimate investigations to protect people, including many of our users, against all forms of criminal activity. To that end, we engage with numerous law enforcement agencies and respond to valid legal orders consistent with what is permitted pursuant to applicable and controlling laws. At the same time, our companies, along with most governments, strongly believe law enforcement interests must be balanced against the privacy rights of our users.

It is critical that users have confidence in the safety and security of the Internet and new technologies as their public services, banking, and consumer behaviour is increasingly digitised. It is the goal of both governments and the technology industry to foster innovation and economic growth in the global economy. To do so we must earn and maintain user trust, and users expect that their personal communications be treated with the same respect online, as they would be offline. In response to our users concerns about privacy and their desire to understand how we respond to government requests, we have all committed to publishing transparency reports about our disclosures to law enforcement agencies around the world. We believe that governments should also be more transparent and agree with the Interception of Communications Commissioner that the current statistical information available to the public is inadequate. We also believe in strong, well-resourced accountability and bodies that ensure law enforcement and

intelligence agency powers are exercised within the boundaries defined by Parliamentary primary legislation.

The framework of Parliamentary legislation around data collection, whether directly from service providers or as data transits networks and intermediaries, should limit surveillance to specific, known users for lawful purposes, and should not permit bulk data collection of Internet communications. Legislation should be narrowly tailored so as not to interfere with the fundamental rights of citizens, or the freedom of companies to provide services within the European Union or elsewhere. The Government advocates for a robust EU legal framework on data protection that safeguards users and is workable for international business, and this commitment must also extend to the legal framework around the collection of communications data and surveillance.

The practical and operational challenges articulated by the Government are not unique to the UK. They are global problems and require a global solution. Attempts by individual governments to address this challenge through unilateral action and new local laws do not provide a sustainable approach. Instead they often create conflicts of law which add to, rather than diminish, the challenges. Moreover, unilateral jurisdictional action will impact economic growth as such action will lead to a fragmentation of the global Internet. There are long established processes for conducting cross-border investigations, such as Mutual Legal Assistance Treaties (MLAT), and instead of jettisoning those entirely governments should focus their energy on improving those processes or developing a new international framework.

This framework should be robust, principled and transparent and govern lawful requests for communications data and surveillance across jurisdictions. Governments should not unilaterally try to compel disclosure of email or other private content across international borders, particularly when that data belongs to citizens of another country. An approach that protects individual rights and privacy, the legitimate interests of law enforcement, and the laws of other jurisdictions would provide the most sustainable legal framework and be worthy of emulation by governments around the world. Such processes must be governed by adequate legal process and oversight but not hampered by undue bureaucratic delays.

We believe that the UK can take the lead internationally by developing a new approach to policy making in this area that would secure trust in governments and protect the future of the Internet as a place to access services, do business, gain education and communicate globally. Our companies, among others, have developed a set of global principles to reform government surveillance through the Reform Government Surveillance Coalition. We believe that, if followed, these principles allow governments to legitimately investigate crime while protecting user trust in the web. We outline these principles below as we hope they will be helpful for you to consider during this Review and we look forward to participating fully in this process.

Reform Government Surveillance Principles:

1) Limiting Governments' Authority to Collect Users' Information

Governments should codify sensible limitations on their ability to compel service providers to disclose user data that balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the Internet. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications.

2) Oversight and Accountability

Intelligence agencies seeking to collect or compel the production of information should do so under a clear legal framework in which executive powers are subject to strong checks and balances. Reviewing courts should be independent and include an adversarial process, and governments should allow important rulings of law to be made public in a timely manner so that the courts are accountable to an informed citizenry.

3) Transparency About Government Demands

Transparency is essential to a debate over governments' surveillance powers and the scope of programs that are administered under those powers. Governments should allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose this data publicly.

4) Respecting the Free Flow of Information

The ability of data to flow or be accessed across borders is essential to a robust 21st century global economy. Governments should permit the transfer of data and should not inhibit access by companies or individuals to lawfully available information that is stored outside of the country. Governments should not require service providers to locate infrastructure within a country's borders or operate locally.

5) Avoiding Conflicts Among Governments

In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty - or “MLAT” - processes. Where the laws of one jurisdiction conflict with the laws of another, it is incumbent upon governments to work together to resolve the conflict.

Faculty of Advocates

Last week, the press contained reports on access by the security services to lawyer-client communications. In light of those reports, I have written to the Advocate General for Scotland, seeking clarification of the current position. I write to you on the same subject in the context of the Review which you are currently undertaking.

I know that I need not stress to you the importance which attaches to the principle of lawyer-client confidentiality. The Code of Conduct for European Lawyers, to which the Faculty of Advocates adheres, puts it this way:

> "It is of the essence of the lawyer's function that the lawyer should be told by his or her client things which the client would not tell to others, and that the lawyer should be the recipient of other information a basis of confidence. Without the certainty of confidentiality there cannot be trust. Confidentiality is therefore a primary and fundamental right and duty of the lawyer. The lawyer's obligation of confidentiality serves the interest of the administration of justice as well as the interest of the client. It is therefore entitled to special protection by the State."

The Edward Report, *The Professional Secret: Confidentiality and Legal Professional Privilege in the Nine Member States of the European Community,* prepared for the CCBE (the Council of European Bars and Law Societies) in 1975 by Sir David Edward, explains matters thus:

> "The purpose of the law is not the protect the lawyer or his individual client. The purpose is, first, to protect every person who requires the advice and assistance of a lawyer in order to vindicate his rights and, second, to ensure the fair and proper administration of justice. This cannot be achieved unless the relationship between the lawyer and his client is a relationship of confidence. The rights, duties and privileges given to lawyers are therefore an essential element in the protection of individual liberty in a free society. They exist for the public interest; they have not been created by lawyers for their private benefit."

There has, in the last year or so, been profound disquiet amongst the legal professions across Europe about the risk which the work of the security services may pose to this core value of the profession – and hence to the rule of law itself. I am sure that you will have seen the CCBE's statement issued in October 2013 about mass data mining,

which expressed "deep concern that a core value of the profession...is at serious risk, and erosion of this aspect of confidentiality will erode trust in the rule of law". I attach a copy for your convenience. The CCBE has expressed the opinion that the issue goes beyond the risk to specific human rights between private persons, but "is a threat to the rule of law as recognised in modern democracies".

The CCBE statement also explains the acute dilemma which the present situation may present for lawyers – who are obliged to protect client confidentiality - as regards the use of electronic communications. If there are not in place robust safeguards – technical and procedural - for lawyer-client privilege, then not only may confidence in the rule of law be undermined, but lawyers may be forced to address whether their use of methods of communication which put their clients' confidences at risk. As the leader of one of the UK's legal professions, I view the issue with great concern not only because of the constitutional importance of lawyer-client confidentiality, but also because of these practical implications.

I hope that the propositions which I have set out above will not be controversial. Earlier this year, the Director of the US National Security Agency wrote this in a letter to the American Bar Association: "NSA is firmly committed to the rule of law and the bed rock legal principle of attorney-client privilege ... We absolutely agree that the attorney-client privilege deserves the strong protections afforded by our legal system, and that it is vital that proper policies and practices are in place to prevent its erosion." I would hope that the United Kingdom Government and the United Kingdom security services will take the same view.

I note that your remit includes safeguards to protect privacy. I am sure that in that context you will be considering specifically the position as regards lawyer-client confidentiality. By reason of the constitutional dimension of lawyer-client confidentiality, this requires, I would suggest, specific and special protection. There require to be robust procedural and technological safeguards in place for lawyer-client confidentiality. As a matter of principle, if there is to be any limitation on or qualification of lawyer-client confidentiality (and I should not be taken as accepting that there should), that should be dealt with by express legislative provision, and should be the subject of explicit and transparent safeguards. The matter is too important to be dealt with only by way of the internal policy of the security services.

I hope that, although the Faculty of Advocates did not submit evidence before the deadline for evidence to your Review, these brief observations on this specific subject will be useful to the Review. I would be glad to provide further amplification should that be of assistance.

James Wolffe QC
November 2014

Links to attachment referred to in the submission:-

http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_14142013_CCBE_Sta1_1382086457.pdf

http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_04042014_Comparat1_1400656620.pdf

Gambling Commission

Thank you for the opportunity for the Gambling Commission (the Commission) to contribute to the review of communications data and interception powers. We have provided answers to the questions as requested, refreshing our material earlier provided to the government when they were concerned with the draft Communications Data Bill.

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

The Gambling Act 2005 established the Gambling Commission specifically to be the expert body responsible for gambling regulation in Great Britain as well as the adviser on gambling matters to government. The Commission is under a duty, under the Gambling Act 2005, to pursue the three licensing objectives set out in section 1 of the Act:

- Preventing gambling from being a source of crime or disorder, being associated with crime or disorder or being used to support crime.
- Ensuring that gambling is conducted in a fair and open way.
- Protecting children and other vulnerable persons from being harmed or exploited by gambling.

The British gambling industry operates in a national and increasingly global context. The 2012 Gross Gambling Yield (GGY)[1] of licensed and regulated gambling is assessed at $430billion, expected to rise to $470 billion in 2014. Europe accounts for 41% of global betting GGY, with the UK having the second largest national betting market.

The regulated British gambling industry generated last reporting year a GGY of £6.7 billion. The industry makes important contribution to the economic well being of the UK economy, directly employing in excess of a hundred thousand adults.

Advances in technology are driving industry product innovation and enabling widespread international access. This is now facilitating the provision of a wide range gambling services from traditional on-course betting operators and betting shops, casinos, bingo halls and arcades to global operators utilising diverse remote distribution channels, including the internet and other means of electronic or distance communication such as mobile phone and communication technology and digital TV requiring increasingly sophisticated linked gambling and financial transaction capabilities.

The crime related threats relevant to the Commission's purpose and the potential use of communications data are:

- The provision of illegal gambling, from within GB and other jurisdictions.
- Organised crime gaining control of licensed gambling operators.
- Organised and individual criminals using gambling to launder money, including disposal of the proceeds of crime.
- Organised crime subverting licensed operators controls to generate criminal profit from the manipulation of sporting events.

[1] Gross Gambling Yield is the total stakes plus the total other amounts accruing to the licensee minus amounts for the provision of prizes or winnings.

In regards to the risks we face, given the significant sums of money being transacted on a daily basis, organised and opportunistic criminals will, we believe seek ever sophisticated ways to generate criminal profit through the corruption or exploitation of gambling in both remote and non remote forms, in national and international contexts.

Significant changes to Great Britain's remote licensing regime are imminent, wherein all gambling provided to consumers within Great Britain will require a Gambling Commission licence, irrespective of where they are located. This creates a requirement for the Gambling Commission to investigate the suitability of all applicants and identify and act against those providing gambling facilities illegally, wherever they are located. This represents a likely significant increase in investigative work requiring communications data given that at present only approximately 15% of remote operators providing facilities are required to be licensed by the Commission.

The targeting of the British gambling market by those operating illegally will produce a range of associated harms, ranging from the provision of a safe and fair betting market for British consumers, commercial sustainability and affect employment and tax revenues. Further, the interests of British sport will be put at risk of compromise due to the likelihood of increased corrupt sports betting activity as will the Britain's reputation for effective gambling regulation and our national capability to address gambling related crime.

The Gambling Commission has powers of prosecution for offences against the Gambling Act and as such has intelligence and investigation capability. In addition the Commission has specific responsibility with regard to supporting the national approach to combating what is commonly referred to as 'match fixing' wherein sport events are manipulated to provide opportunity to successfully bet.

Information and intelligence (received from betting operators, law enforcement, public and sports) is managed through the Commission's secure intelligence function and referrals relating to suspected corrupt sports betting through the Commission's Sports Betting Intelligence Unit (SBIU). The intelligence function processes high quality intelligence about illegal activity, and undertakes preliminary investigations into the corrupt activity of identified match-fixers, complementing reports of suspect betting on particular sports events reported by the betting industry. The Commission's trained investigators and case managers are supported by the Intelligence/SBIU when conducting investigations into suspected criminal activity and in particular by acting as the secure single point of management for all Data Communications enquiries. The loss of the ability to gain communications data effectively and efficiently will undermine our criminal intelligence and investigation capability and would likely lead to the requirement for police forces or a law enforcement agency to assume the investigation role in many cases.

Reallocation of SBIU responsibilities will have both national and international implications. The SBIU has been instrumental in protecting UK interest by developing international cooperation arrangements to combat 'match fixing' and related organised criminality. The current national approach to tackling this threat, agreed with government, the Association of Chief Police Officers (ACPO),National Crime Agency (NCA), sports governing bodies and licensed betting providers, will have to be re considered. The costs presently borne by the Commission (funded by license fees) would likely fall to police/taxpayer.

2. 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.

***

3. 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?

We anticipate the activities of those looking to criminally exploit gambling as a source of criminal profit will diversify and increasingly operate within the cyber environment. The significant challenges will arise in tackling enterprises emanating from a variety of UK and overseas jurisdictions, using a variety of technologies, fraudulent or false identities seeking the anonymity that the internet can provide. We perceive there are increased risks of direct financial loss by consumers and legitimate operators and compromise of confidence in industry security which will be immediate and difficult to recover.

Areas of specific concern relate to the developing use of cloud services (in particular our ability to trace data and user locations) and questions as to who owns the data in networked systems and how long will they retain the information pose challenge for the evidence gathering process. We are also alert to the increasing investigative challenges of dealing with individuals hosting forums on their own servers, using peer to peer networks, virtual private networks (VPN) and global sensor technology.

We are encountering those suspected of involvement in betting integrity issues using Wi-Fi enabled technology and multiple platforms to communicate, increasing the challenge of establishing who is involved in potential conspiracy or other criminal activity.

Overall we feel the risks will continue to develop in the areas outlined in question one; the Commission needs access to relevant communications data to avoid significant intelligence and evidential gathering gaps compromising our ability to undertake enquiries into unlicensed gambling and other criminal activity. It is difficult to see how the Commission could discharge its functions effectively particularly given the expansion of our regulatory remit to identify and regulate all operators providing to British customers based in the UK or overseas and investigate betting integrity without the power to acquire communications data when necessary.

4. 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?

Our intelligence and investigation activity in both remote and non remote contexts shows there are few alternative methods to obtain the intelligence and evidence as provided by

communications data. Given that the Commission is predominantly investigating events that have occurred, communications data is often the only way to comprehensively capture the necessary evidence of the retrospective conspiracy.

Alternatives such as directed surveillance are less effective, less efficient and more intrusive and loss of our ability to access communications data would result in requests for additional police assistance and incur delay and significant additional costs for both Commission and police. We know that gambling related criminality is not a priority for the police and the Commission acts as the lead agency in this area and loss of communications data would seriously compromise our capability to discharge our function

The loss of the capability would leave the Commission facing a situation of having to consider the need to request the voluntary sharing of communications data by those we suspect of acting illegally, with no compulsion on their behalf to cooperate. We would not be able to identify with whom they were communicating other than through their disclosures nor be able to corroborate if they were telling the truth. This process would be protracted, ineffective and resource intensive.

Further as we are often trying to identify unknown principals to a crime, we would have to approach the holders of communications data to share more limited information on a voluntary basis within the framework of the Data Protection Act. We do not consider that these arrangements would deliver the evidence necessary to show the complex communications used by those in criminal conspiracies, thus weakening the evidential base for prosecution.

We are aware of the use of open source research and commercial databases to identify connections between data and individuals and already use prior to requesting communications data. It has provided limited information, insufficient in itself to develop sufficient intelligence and is often non evidential in nature.

An alternative would be to ask the police to assume gambling related criminal investigations in addition to having impact upon capability of the Commission to discharge its core functions it would represent a significant transfer of responsibility and associated cost to the police/taxpayer, almost certainly resulting in a loss of intelligence capability and investigative expertise and some difficult decisions as to which force and under what circumstances would individual investigations be allocated. We can identify no benefits to these alternative arrangements.

The loss of access to communications data and transfer of responsibility to law enforcement or police would likely leave the Commission to be capable of prosecuting only those who chose to self incriminate. The consequence of these changes would likely result in increased risk of harm to the public and a proliferation of crime associated to gambling.

With very significant sums of money being transacted in the gambling environment every day, organised crime and those who wish to take advantage of individuals will seek to corrupt or exploit the provision of gambling particularly if the risk of being detected is perceived of as being low.

The current Commission-led response has we believe proven itself to be effective and efficient in controlling crime related to gambling, safeguarding communities and protecting children and vulnerable customers from being exploited.

5. 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 and the period of time for which the information should be available before the request to examine it.

***

6. 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 information you are examining?

The Commission became fully operational in September 2007. Since then our ability to acquire communications data has been highly valued and we believe delivers significant benefits for the public. We are recognise as the leading agency in a specialist area and that gambling related criminality is not a priority for any police or law enforcement agency. We seek and support collaboration with public and private sector and ensure that our decision making is focused upon the primary risks within the Gambling Act.

To this end we have ensured that:

- Our policies and procedures are reviewed and aligned to efficient operational practice.
- Our staff are trained and understand the legislation with regards to investigation and access to communications data,
- Applications to acquire communications data are submitted by investigators through our single point of contact (SPOC) within the Commission's secure intelligence unit, who is trained and accredited to national police standards.
- Suitable applications are considered by one of four senior officers, also trained and experienced in the exercise of functions under RIPA.
- Acquired data is securely held and subject to operational oversight through our management procedures.
- The Commission has been subject to regular robust inspections by the Interception of Communications Commissioner (IOCCO) and assessed as having high standard application and oversight arrangements.

We believe the Commission current arrangements using our designated persons ensure we fully test the proportionality and necessity of our requests for communication data and minimise the intrusion into the privacy of those whose information we are examining.

***

7. 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?

The UK is one of the largest regulated gambling markets in the world, and our sports betting / sporting products are of global interest. The Gambling Commission has regulatory and criminal enforcement powers but operates on the basis that it is the responsibility of operators to be licensed and themselves manage the risk to the licensing objectives created by their

business models. A licensee's suitability is in large part determined by their integrity and competence in managing their regulatory risk alongside their commercial risk.

The approaches to gambling regulation as a means of managing the criminal threats associated with gambling being an attractive source of criminal profit differs considerably between countries. The threats do not differ in any great measure, and the management of the risks are dependent upon the capability of national regulatory arrangements (or prohibition measures where gambling is outlawed) and international collaborations.

I believe The Gambling Commission is considered to be an effective and efficient regulator and is using its criminal enforcement and regulatory powers to best effect. The challenge that we face (and all others) is having the investigative skills and authorities to understanding and evidence the criminal / corrupt connections between people, locations, gambling and sporting events which in a cyber age will increasingly take place through expanding communications technologies.

Nick Tofiluk
Director Regulatory Operations
October 2014

Peter Gill

1. Introduction: This submission is made in my personal capacity as Honorary Senior Research Fellow, at the University of Liverpool. It addresses four of the questions identified in the Review's Objectives: the case for amending or replacing legislation, the statistical and transparency arrangements that should apply, issues of privacy in relation to encryption and the effectiveness of the current oversight arrangements.

2. Does Part 1 of RIPA need amending or replacing?

2.1 All intelligence-related legislation – Interception of Communications Act 1985 (IOCA), Security Service Act 1989 (SSA), Intelligence Services Act 1994 (ISA), Police Act 1997 (PA), Regulation of Investigatory Powers Act 2000 (RIPA) - both empowers and limits the agencies. To a greater or lesser extent, all this legislation reflects government attempts to come to terms with, first, the European Convention on Human Rights (ECHR) and then the Human Rights Act 1998 in a field of state policy – national security – where executives always seek to maintain the maximum discretion for themselves in implementing security policy. For example, UK law says what information governments *may* collect regarding national security 'with particular reference to', for example, serious crime and economic wellbeing but they do not specify what they may *not* collect, for example, information on lawful, peaceful political activities. Arguably, it is time for a statutory definition of 'national security'.

2.2 It is generally acknowledged that the law has *always* lagged behind developments in communications technology and, to the extent that the latter takes place at increasing speed, this problem grows. The RIPA framework seems to have served the agencies well, if we are to believe government statements that they have acted legally: former GCHQ Director and the architect of RIPA as Home Office Permanent Secretary, David Omand said that 'For Britain, Snowden's public interest justification is thin since subsequent investigation has shown conclusively (that GCHQ) has at all times acted lawfully.'[1] But these reassurances are somewhat weakened by the report that one of GCHQ's 'key selling points' in its financially subsidised relationship with NSA is the UK's more relaxed legal regime.[2]

2.3 But the current law is obscure and has not contributed to public understanding. Even David Omand acknowledges this, as he told the Home Affairs Committee:

'The instructions to parliamentary draftsmen were to make it technology-neutral, because everyone could see that the technology was moving very fast. Parliamentary draftsmen did an excellent job in doing that, but as a result I do not think the ordinary person or Member of Parliament would be able to follow the Act without a lawyer to explain how these different sections interact.'[3]

But even senior lawyers struggle: the Interception of Communications Commissioner (IoCC), a former judge in the Court of Appeal, describes some of the provisions of RIPA Part 1 as 'difficult for anyone to get their head round…'[4] and notes that 'a reader's eyes glaze over before reaching the end of Section 1, that is, if the reader ever starts.'[5]

2.4 RIPA was passed in order to ensure that authorisation procedures for all forms of covert information gathering would pass muster before the courts as adequate protection of ECHR s.8

[1] David Omand, 'Edward Snowden's leaks are misguided…' *The Guardian*, September 26, 2013.
[2] 'Inside GCHQ…' *The Guardian*, August 2, 2013, 1-2.
[3] February 11, 2014, Q589
[4] IoCC, 2014, *2013 Annual Report of the Interception of Communications Commissioner*, para. 6.5.3.
[5] IoCC, 2014, para. 6.7.2.

privacy rights in the light of the Human Rights Act 1998 (which came into effect in 2000) and to update the law on interception. IOCA had been passed in order to legalise interception when the longstanding UK practice of ministerial authorisation alone had been found to be in breach of the ECHR.[6] Typifying the minimal approach to 'legalising' covert surveillance at the time, IOCA only referred to telephone tapping, 'metering' (collecting what would later become known as communications or meta-data relating to the sender and recipient of calls) and mail interception. It did not cover, for example, electronic surveillance ('bugging') which was legalised for the Security Service in the SSA and for police in the Police Act 1997. Also, since IOCA referred only to mail and telephone interception, it was outdated and could not deal with the Internet.

2.5 RIPA retained the distinction - established in IOCA - between a warrant for interception of named people and places under s.8(1) and a 'certificated' warrant under 8(4).[7] The former targets the 'knowns' whose name(s), address(es), telephone number(s) are specified but the s.8(4) 'certificated' warrant seeks the 'unknowns' through the interception of 'external communications'[8] if

> 'at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying (i) the descriptions of intercepted material the examination of which he considers necessary; and (ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c) (that is, in the interests of national security; for the purpose of preventing or detecting serious crime; or for the purpose of safeguarding the economic well-being of the United Kingdom).'

2.6 It is these 'certificated' warrants that have proved so controversial since they are the basis for the bulk collection of communications and then their examination seeking specific 'selectors' or keywords in communications that can be subject to further analysis. For example, we have learnt that GCHQ collects material from the cables as they come ashore from the Atlantic in an operation named 'Tempora'. Thirty per cent of the massive volume of communications is immediately rejected while 40,000 'selectors' chosen by GCHQ and 31,000 by NSA based on key words, phone numbers etc. trawl the rest. A programme called TINT then facilitates storage permitting retrospective analysis by the 300 GCHQ and 250 NSA analysts working on 'target discovery' and 'target development'.[9]

2.7 Little or no effort was made by governments or officials to explain this searching process to the public. The Commons' debates about RIPA in 2000 did not examine the issue even though there was a contemporaneous debate in Europe sparked by the exposure of the NSA's *Echelon* programme in which transatlantic satellite communications would be searched by means of a 'dictionary' of keywords so that the messages containing them could be further interrogated.[10] While the examination of external communications is entirely legitimate foreign intelligence gathering, it was inevitable that, given the mixing of external and internal communications in routing *via* the Internet, agencies would automatically gather both.

2.8 This point was made during the Lords' Committee discussions by an Under Secretary of State for the Home Office[11] yet the RIPA Code of Practice maintained that external communications 'do not include communications both sent and received in the British Islands, even if they pass outside

[6] *Malone v UK* (1984) 7 EHRR 14.
[7] Cf. Victoria Williams, 2006, *Surveillance and Intelligence Law Handbook*, Oxford UP, 74-75. GCHQ reportedly have 10 basic certificates that cover the entire range of their intelligence production. 'Legal loopholes…' *The Guardian* June 21, 2013.
[8] '…a communication sent or received outside the British Islands.' RIPA. s. 20. See detailed discussion below.
[9] http://www.guardian.co.uk/world/the-nsa-files?INTCMP=SRCH See articles dated June 21, 2013.
[10] Duncan Campbell, *Interception Capabilities 2000*, Report to European Parliament's Science and Technology Options Assessment Panel (STOA) May 6, 1999.
http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf
[11] Lord Bassam of Brighton, July 12, 2000, *Hansard* col. 323 cited in Witness Statement of Charles Blandford Farr, 2014, para.130. https://www.amnesty.org.uk/sites/default/files/witness_st_of_charles_blandford_farr.pdf June 25, 2014.

the British Islands *en route*.'[12] Therefore, once intercepted, those communications between people *within* Britain could only be analysed on the basis of a s.8(1) targeted warrant. However, a year after the disclosure of NSA and GCHQ files began, Charles Farr's[13] statement to the Investigatory Powers Tribunal (IPT), responding to Amnesty International's case challenging GCHQ practices, indicated how RIPA has been interpreted by government to permit, in essence, the analysis of any communication, external or internal.

2.9 There are two distinct dimensions to this: first, while an email from someone in Leicester to someone in Liverpool may well be routed through servers outside the UK, it is an internal communication for the purposes of RIPA and, even if 'collected', may not be 'examined' without a s.8(1) warrant.[14] Second, however, if someone in Leicester or Liverpool searches on Google, YouTube or posts a message on Facebook, then the recipient is deemed to be the relevant servers, usually outside the UK, the communications are therefore 'external' and consequently *are* subject to examination under 8(4). However, it now appears that under 'strictly limited circumstances'[15] a s.8(4) warrant may permit the analysis of a communication between two people *within* the UK if the ministerial certificate deems it 'necessary' in the interests of national security, prevention of serious crime or economic wellbeing under RIPA s.5(3 a-c) and it relates to a period of no more than three months of interception.[16]

2.10 Prior to June 2013, no enlightenment on any of this came from oversight by the Interception of Communications Commissioner (IoCC).[17] His 2004 Report (pp.8-9) cited an IPT decision of December 2004 upholding the lawfulness of an 8(4) warrant but there was no explanation of the significant differences between the two types of warrant. The 2010 Report (p.10) provided a graphic of the warrant authorisation process but this also made no reference to the two types of warrant. Now it is reported that GCHQ activities are covered by just ten s.8(4) certificates, we can see this is a very significant omission. The IoCC's 2013 Annual Report does provide more information on 8(4) warrants: the 'selectors' must be 'referable to individuals'[18] and elsewhere the Report refers to 'search criteria constructed to comply with the s.8(4) process'.[19] Therefore, in seeking to counter the claims of indiscriminate trawling of the Internet, the IoCC is anxious to maintain that searching is about seeking (presumably suspected) individuals (and those in contact with them) but it seems that the task for agencies in seeking warrants is to 'construct' the application in such a way that it can be seen to 'refer' to individuals. Clearly the IoCC does not want to be more explicit for fear of compromising methods but, elsewhere, more information has been given on this crucial process without apparent damage (see below).

2.11 Overall, it appears that the reason for official insistence that GCHQ has acted lawfully, while critics argue the opposite, lies in the broad powers in RIPA s.8 when combined with ISA s.3 which mandates GCHQ 'to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material…' If the law does not require up-dating, it certainly requires clarification and better explanation as well as improved oversight of those who apply it.

[12] Home Office, *Code of Practice for the Interception of Communications*, September 8, 2010. https://www.gov.uk/government/publications/code-of-practice-for-the-interception-of-communications
[13] Director General of the Home Office's Office for Security and Counter-Terrorism (OSCT)
[14] Cf. Farr, 2014, para.129.
[15] Farr, 2014, para.158.
[16] RIPA s.16(3). The Terrorism Act 2006 s.32 (6) increased the period to six months for 'national security'.
[17] See IoCC annual reports, especially re. RIPA Chapter 1, for 2000-2012; 2001 and 2009 could not be downloaded. http://www.iocco-uk.info/ January 20, 2014
[18] IoCC, 2014, 6.5.38
[19] IoCC, 2014, 6.5.43

3. What statistical/transparency requirements should apply?

3.1 President Obama's Review Group wondered whether artificial intelligence software could be developed to enable selective collection in real time rather than requiring storage and subsequent sorting but they admitted they had no idea whether the concept was 'feasible or fantasy'.[20] If governments believe it is necessary to store 'everything' (even if for only 30 days, in order to permit searching *via* selectors) then they need to explain to the public why this is so and establish clear procedures to monitor the process in order to allay public concern. For example, governments have a legitimate need to search data retrospectively in order to investigate the networks of current suspects and for those currently 'unknown'. On the other hand, the attempt to 'collect everything' is arguably so disproportionate to current security and criminal threats that it requires more robust oversight than is provided by the current UK structure (see further below).

3.2 For example, it is entirely possible to explain these processes without threatening security: the Dutch Review Committee on the Intelligence and Security Services (RCISS) has provided a useful account of why and how selection criteria including key words are used to filter bulk collection. Ministerial permission is granted for a general subject to which the key words are related but not for the precise lists of key words which may be amended daily as necessary. 'Generic identities' are also used and cover a particular 'type' of person or organisation and avoid the need to identify specific individuals. The advantages for the agencies are obvious: the specific names and locations of individuals may not be known, organisations change their names, and people use aliases and multiple channels of communication.[21]

3.3 Communication Service Providers (CSPs) should be empowered to disclose the numbers of requests/orders for disclosure and number of users whose information is produced. It would still be against the law to reveal individual requests but a presumption of transparency is central to democratic security governance and this can only be rebutted if the efficacy of the programme would be substantially damaged if it were disclosed. The US Government has changed its policy so that the broad range of requests can be published, for example, January - June 2013, between 9,000-9999 Google user accounts were the subject FBI or FISA requests. [22]

4. Privacy and encryption

4.1 But after collection, the problem for the agencies is the ubiquity of encryption. GCHQ started life in the early twentieth century as the Government Code and Cypher School and has been in the business of code-breaking ever since.[23] With the advent of commercially-available high quality encryption, RIPA Part III attempted to deal with the increasing challenge of interception by requiring CSPs to supply information in unencoded form or to supply the key required to 'unlock' it. They could face criminal sanctions for non-compliance and/or for disclosing the fact that a disclosure notice had been served.[24] Beyond this procedure, the Snowden documents reveal a set of highly controversial state-corporate relationships. We learn of the insertion of backdoors or trapdoors into CSPs software, either with or without their knowledge. Although the companies

[20] *Liberty and Security in a Changing World*, December 12, 2013, 173-74 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf January 20, 2014

[21] Review Committee on the Intelligence and Security Services, 'On the use of Sigint by DISS,' *Annual Report* 2011-12, 37-110 at 88-98. http://www.ctivd.nl/?English January 20, 2014.

[22] 'Vodafone takes a stand…' *The Guardian,* January 16, 2014, 2: Vodafone writing to UK ministers asking for right to disclose number of demands it receives for data. USG has just changed its policy so that the broad range of requests can be published, for example, January - June 2013, between 9,000-9999 Google user accounts were the subject FBI or FISA requests. *Reuters*, February 3, 2014.

[23] Richard J. Aldrich, *GCHQ: the uncensored story of Britain's most secret intelligence agency, London*, Harper*Press*, 2011.

[24] Williams, *Surveillance and Intelligence Law Handbook*, 2006, 195-203.

deny that they cooperate, if they do, their motivation is presumably a mix of the patriotic and the financial.[25] But where company cooperation is not forthcoming or there is no CSP within legal range, GCHQ continues to 'crack' codes through computing power and also deploys a Humint Operations Team for recruiting and running covert agents within CSPs.[26]

4.2 The legality of such operations seem to be assured by ISA s.3 which says it is one of GCHQ's functions to 'provide information…derived from encrypted material' taken together with RIPA s.5(6):

'The conduct authorised by an interception warrant shall be taken to include – *all such conduct* (including the interception of communications not identified by the warrant) as is necessary to undertake in order to do what is expressly authorised or required by the warrant.' (emphasis added)

Legal empowerment does not come much more all-embracing than that!

4.3 But there is now evidence that some CSPs are less prepared to cooperate with governments, just as more foreign governments seek to get in on the act by demanding data.[27] Facebook is challenging US prosecutors' warrants for all the account data for 381 people in pursuance of a fraud against Social Security.[28] The CSPs and other US companies also fear reputational damage, for example, the German Interior Ministry has dropped a contract with Verizon as the German government tries to increase information security.[29] In the UK GCHQ's hacking and use of malware is the subject of a legal challenge by Amnesty International *et al* before the IPT.[30] There has been much criticism of the agencies attack on encryption because, it is argued, it renders the software more vulnerable to other hackers and threatens its integrity for all computer users.[31] Tim Berners-Lee, founder of the world wide web, is especially critical, saying it was foolish, contradicted the government's fight against cybercrime, and betrayed the technology industry.[32]

4.4 State-corporate interaction comes under the purview of the IoCC and he has reported on occasional meetings with CSPs to discuss their operations but discussion of these matters elsewhere has revealed a glaring gap in the oversight regime. The Telecommunications Act 1984 (TA), passed to privatise telecommunications services, had to deal *inter alia* with the issue of how state agencies could insist on the continued cooperation of *private* corporations in their interception activities. S. 94 accordingly empowered the Secretary of State to direct 'providers of public electronic communications networks' to do whatever was deemed necessary and proportionate 'in the interests of national security or relations with the government of a country or territory outside the UK.' The minister might also direct that nothing could be disclosed about these arrangements and is under no obligation to inform Parliament about them if he believes disclosure would be against the interests of national security or relations with the government of a country or territory outside the UK. Whether RIPA s.12 or TA s.94 is the main source of the extensive state-corporate relations in this field is not known but the latter lacks any mechanism for oversight at all; none of

[25] E.g. Dominic Rushe, 'Yahoo and Microsoft express alarm over NSA attacks on online security,' *Guardian*, September 7, 2013, p.2
[26] 'Exclusive: how US and Britain unlock privacy on the internet,' *The Guardian*, September 6, 2013, pp.1, 4-5. See also ISCommr, *Annual Report for 2013*, p.34. June 26, 2014.
http://isc.intelligencecommissioners.com/sections.asp?sectionID=1&type=top
[27] 'Internet Giants Erect Barriers to Spy Agencies,' *New York Times* June 6, 2014.
[28] 'Forced to Hand over Data…' *New York Times,* June 26, 2014
[29] 'Berlin drops Verizon over US spying fears,' *Financial Times*, June 26, 2014
[30] 'GCHQ spying programs face legal challenge,' *The Guardian*, May 14, 2014, 12
[31] E.g. 'Legislation seeks to bar NSA tactic in encryption,' *New York Times*, September 6, 2013; 'Academics criticise spy agencies,' *The Guardian*, September 17, 2013.
[32] 'Father of the web condemns spy agencies,' *The Guardian,* November 7, 1-2.

the Intelligence and Security Committee (ISC), IoCC or Intelligence Services Commissioner (ISCommr) see it as within their mandate.[33]

5. Are current statutory oversight arrangements effective?

5.1 If democracy and the rule of law are to be sustained when such extensive powers are granted to state agencies, external oversight must be robust and well-resourced. Marginal changes to the powers of the ISC were made by the Justice and Security Act 2013 but in essence the architecture in UK is that essentially 'bolted on' piecemeal during 1985-94 to a structure of agencies in development for over 100 years. Former Lord Chancellor Lord Falconer said that the Snowden material raised very serious questions about the adequacy of this legal framework for oversight of the intelligence services' work in relation to the interception of communications.[34] But the inadequacies revealed by recent controversies go wider; for example, the failure to prevent or expose the human rights abuses involved in the undercover policing of environmental protest movements.[35] This submission argues that the time is ripe to replace the current patchwork approach with a systematic structure for the authorisation and oversight of covert measures.

5.2 The principal oversight tasks are to monitor, audit, investigate, review…

- **legality** and **propriety** of intelligence activities including conformity with human rights conventions;
- compliance with government **policy** and agencies' **effectiveness**;
- **efficiency** of the agencies and their **expenditure**;
- citizens' **complaints**;
- the **entire intelligence community.**

5.3 The core of any oversight system should be a parliamentary committee in order to reflect parliamentary sovereignty. In many countries, including UK, different aspects of the oversight mandate are covered by some mix of parliamentary and extra-parliamentary bodies. Members of parliamentary oversight bodies should be cross-party and appointed by parliament. Members of extra-parliamentary bodies may be appointed by parliament (e.g. Belgium), by government in consultation with opposition (e.g. Canada) or by government from a list of potential members decided by parliament (Netherlands). Where there are different oversight bodies, their mandates should be complementary and overlap should be avoided.

5.4 When implemented, the reforms of ISC introduced in 2013 will increase the research resources available and the committee's access to primary material in the agencies. The Committee will report directly to Parliament, rather than to the PM, though the latter's right to redact sensitive material will remain.[36] Since this procedure leads (rightly or wrongly) to the belief that the PM 'censors' ISC reports, it would be preferable if the Committee itself was to determine the final version of its Reports after its customary consultation with the Agencies. Since the committee may now select its own chair, it would also increase parliamentary and public confidence if it were to adopt the practice of appointing a member of the Opposition.

[33] Home Affairs Committee, *Counter Terrorism*, HC231, May 2014, para. 175. http://www.parliament.uk/business/committees/committees-a-z/commons-select/home-affairs-committee/inquiries/parliament-2010/co-ordinating-the-fight-against-international-terrorism/
[34] 'Security chiefs "exaggerated"…' *The Guardian* November 18, 2013, 1-2.
[35] Rob Evans & Paul Lewis, 2013, *Undercover*, Faber & Faber.
[36] ISC *Annual Report for 2012-13*, paras 127-28.

5.5 Hitherto, the UK system has been characterised by an unfortunate 'compartmentalisation' in which each body works essentially alone; yet the resources for oversight are scarce and should be leveraged for greatest effectiveness. In recent years the ISC has started to have an annual meeting with commissioners but there are greater opportunities. For example, there are other parliamentary committees with an interest in intelligence matters, though without ISC's access, and it would assist the overall impact of parliamentary oversight if ISC were to cooperate with other committees rather than seeing them as competitors.[37]

5.6 The other main reason why ISC must seek a broader range of partners is the overarching significance of intelligence cooperation both between state and corporate sectors and transnationally. State-corporate relations in communications interception are extensive and without them states would be 'deaf' but there are clear dangers that, if abused by states, companies may withdraw cooperation or may themselves suffer reputational damage. This may be primarily a problem for shareholders but the interdependence of states and corporations means that oversight bodies must take an interest.

5.7 Similarly, recent revelations remind us that international intelligence cooperation is almost entirely secret and not subject to law. First, the only limit on the transfer of information abroad by UK agencies is ministerial discretion (RIPA, s.15). There is no restriction on the receipt of information from abroad (except in the case of torture). Second, cooperation is usually bilateral and any subsequent action is more likely to be disruptive than aimed at arrest and prosecution. Third, although there are formal intelligence-sharing agreements, much cooperation takes place informally between practitioners. Fourth, intelligence sharing is subject to the 'control' principle whereby an agency may not disclose intelligence to a third party without the permission of the originating agency. This may be applied also to external oversight bodies. So, it is important not only that the ISC continues to cooperate with Biennial Conferences of Intelligence Review bodies but also encourages such initiatives as the European Network of National Intelligence Reviewers.[38]

5.8 But while parliamentary committees are *necessary* for democratic oversight they are not *sufficient* to make it effective; since June 2013 it has become clear that there are other serious shortcomings in the UK structure, specifically in the Commissioners and IPT. Currently, the IoCC[39] reviews the warrant issuing process, ministers' and agencies' performance in *interception*, acquiring and disclosing *communications data* and the process by which agencies other than intelligence and military gain access to *encrypted data*. The ISCommr[40] reviews the agencies' procedures regarding warrants for the 'interference with property', electronic surveillance, 'covert human intelligence sources' (CHIS) and the requirement for the disclosure of encrypted data. The ISCommrs' role has been extended since 2009 to include monitoring compliance with the guidelines on detention and interviewing[41] and the Justice and Security Act s.5 amended RIPA so that the PM could direct the ISCommr to review any other specific aspect of the intelligence services including military intelligence. Though responding to allegations of abuse of detainees, this begs the question as to why oversight should wait for a prime ministerial direction. The Office of Surveillance Commisioners (OSC)[42] reviews covert surveillance (entry on/interference with property or electronic surveillance) and CHIS other than by the intelligence services.

5.9 RIPA ss.65-70 rationalised the previous arrangements to address public complaints into a

[37] Cf. Hugh Bochel *et al*, 2013, '"New Mechanisms of Independent Accountability2: select committees and parliamentary scrutiny of the intelligence services,' *Parliamentary Affairs*, advance access, November 13.
[38] http://www.ennir.be/about-the-european-network-of-national-intelligence-reviewers
[39] http://www.iocco-uk.info/ appointed under RIPA 2000 s.57 (originally IOCA 1985)
[40] RIPA 2000 s.59 (originally Security Service Commissioner in SSA and then ISCommr in ISA) http://isc.intelligencecommissioners.com/default.asp
[41] E.g. http://isc.intelligencecommissioners.com/sections.asp?pageID=34&sectionID=5&type=blog
[42] https://osc.independent.gov.uk/ (originally Police Act 1997 s.91) RIPA s.62.

single IPT[43] which has exclusive jurisdiction to hear and adjudicate on ECHR-based claims against public bodies using covert investigation methods. It may hold hearings in public or private and take evidence that would not be admissible in court. Part of the current case brought by Amnesty International *et al* re. Snowden was heard in public in July 2014. From 2001-13 IPT received 1674 complaints of which 10 were upheld (5 from the Poole school catchment area case.)

5.10 Oversight requires a full-time independent expert body: commissioners are former members of the judiciary but they are in retirement and only work part-time. The IoCC and OSC have multi-disciplinary staffs[44] reflecting their broader mandates over police and other public bodies but the ISCommr has only administrative support. **The three commissioners should be combined into a single body that, for convenience, we might call an Inspector General (IG)[45] or a Surveillance Commissioner (SC) with a supporting secretariat of legal advisers and investigators.** There should be a role for the ISC in the appointment of an IG or SC.

5.11 **Mandate.** The ISC mandate – administration, expenditure and policy - could be best balanced by identifying the mandate of the IG/SC as: *legality, propriety and rights*. However, these should not be cast in stone since, clearly, an agency that abuses rights is not 'effective' and one in which financial matters are out of control may be acting illegally. Rather, the specific work programme of the IG/SC should be developed in consultation with the ISC. In this way, both bodies will maximise the impact of their inquiries while avoiding wasteful overlap. While the IG/SC will develop a plan of work for its *proactive* monitoring of intelligence activities, if complaints investigation is added to the remit (as suggested below) then part of its work will be *reactive* to those.

5.12 **Remit: covert investigation techniques**. Arrangements for the oversight of state agencies' use of covert techniques have developed piecemeal since 1985. All forms of covert surveillance are now covered in RIPA but with different regimes, for example, the ISCommr. reviews 'bugging' by the Agencies and the Surveillance Commissioners review that by police while the IoCC reviews interception of communications by all public bodies. Effective oversight can be best achieved by a single body in which experts in the use of all techniques are gathered together to maximise the synergy of scarce resources.

5.13 **Remit: complaints**. These are currently dealt with by the IPT. While it would not be appropriate for complaints investigation to be passed to a parliamentary committee, it would make much sense to have complaints regarding the intelligence agencies investigated by the IG/SC. Experience elsewhere (e.g. Belgium, Canada, Netherlands) is that extra-parliamentary oversight bodies find that the investigation of specific complaints provides a detailed insight into agencies' *modus operandi* and record-keeping and thus reinforces their other review activities. Equally, the broader mandate of these bodies enables them to exercise good judgment as to the significance or otherwise of complaints that are made. The IPT describes itself as 'a judicial body'[46] and, although it has instructed an investigator, relies primarily on the Agencies fulfilling their duty to provide all information requested. The present situation would be improved by the IG/SC investigating complaints and presenting a case to the IPT for adjudication, with or without a hearing.

5.14 **Remit: agency employees**. Since 1987 the Staff Counsellor has acted as an independent outlet for employees with ethical concerns about their work or agencies' activities. Little is known in public as to how effective this has been or how employees view the office. As with public complaints, hearing employee concerns would inform the IG/SC's office regarding difficult issues

[43] http://www.ipt-uk.com/
[44] E.g. IoCC, 2014, para. 6.2.5
[45] Elements of this proposal were made in a submission to the Justice and Security consultation in 2012. The Government response was that this proposal would not really improve on the role of the commissioners. The further shortcomings now revealed and further discussions with colleagues lead me to submit a revised version of that proposal.
[46] www.ipt-uk.com/docs/IPTAnnualReportFINAL.pdf p.34, accessed January 3, 2012

and employees should be able to contact the IG/SC directly. Clearly, in the post-Snowden world, a robustly-independent yet confidential outlet for employees is required.

5.15 **Full Access to people, papers, premises**. It would be appropriate to apply to the IG/SC the standard that is applied to the current commissioners and IPT, that is, it is the duty of agency employees to provide all information requested.

5.16 **Reports**. Reports of the IG/SC into investigations should be made public insofar as possible. The public presentation of annual and specific reports would secure a public face for the IG which, together with the ISC's raised profile, would assist in the key role of public education in this most arcane of government functions. In pursuance of the principle of a cohesive framework for oversight, if confidential annexes are required (or entire reports produced that cannot be made public) then they should be sent simultaneously to the PM and the ISC.

6. Conclusion

The aim of any reconsideration of the legal framework must be to ensure:

a) increased certainty and clarity in the law. Primary legislation cannot be obfuscated on the grounds that it relates to 'national security' or 'sources and methods';

b) the effectiveness and propriety of agency policies and practices; and

c) improved public education.[47] Whatever the disposition of the law, there is a crucial political task for governments and intelligence oversight bodies to explain the limited *reality* of current security surveillance when the *potential* is clearly so vast and threatens public trust.

The objective of reform of the oversight structure must be to increase public reassurance that covert investigations are conducted legally and properly. The scarce resources available for this can best be leveraged by merging the three current commissioners' offices into a single body. This will make the best use of accumulated expertise from the current commissioners while enabling the development of more 'joined-up' oversight.

September 2014

[47] On January 30, 2014 the Prime Minister said to the Select Committee on National Security: 'I do think politicians, police chiefs, the intelligence services have got a role in explaining what this is all about. Snowden inevitably raises questions about "who has access to my data and why" 'PM: my failure to make case…' *Guardian* January 31, 2014, 8.

Global Network Initiative

The Global Network Initiative (GNI) welcomes the opportunity to provide written evidence for the UK Government Review of Communications and Interception Powers. GNI has previously provided evidence to the Joint Committee on the Draft Communications Data Bill and written to the UK Prime Minister concerning the Data Retention and Investigatory Powers Act (DRIPA 2014).[1]

Specifically, we recommend that the UK government:

- Develop reform proposals for lawful interception and communications data that would serve as a worthy model for other countries to adopt, mindful that policy and legislation in the UK is often emulated by governments in the Commonwealth and around the world.
- Halt the bulk collection of content and communications data from providers, and bring all data collection programmes, for law enforcement and national security purposes, under the auspices of an independent oversight regime.
- Prioritize Mutual Legal Assistance Treaty (MLAT) reforms to manage challenges around cross--border data requests, rather than asserting extraterritorial jurisdiction over data controlled outside the UK.
- Adopt a robust set of transparency provisions that enable public understanding of the scope of interception and communications data powers, policies, and practices.
- Broadly consult with industry, civil society organizations, and other key stakeholders to aid in the development of policy options for public debate, informed by human rights impact assessments.

About GNI

GNI is a multi---stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics, working to protect and advance freedom of expression and privacy in the Information Communications and Technology (ICT) sector.[2] GNI has developed a set of Principles and Implementation Guidelines, based on international human

[1] GNI Comments on UK Draft Communications Data Bill, September 2012, available at https://globalnetworkinitiative.org/news/gni-comments-uk-draft-communications-data-bill;

[2] The current list of GNI participants is available at https://globalnetworkinitiative.org/participants/index.php.

rights standards, to guide responsible company action when facing requests from governments around the world that could adversely affect the freedom of expression and privacy rights of users.[3]

The UK's leadership role

The UK plays an important leadership role in the promotion of Internet freedom. Through the Freedom Online Coalition (FOC) and other initiatives, the UK has secured resolutions at the UN Human Rights Council recognizing that the same rights that apply offline also apply online. The UK co---chairs the Coalition working group on privacy and transparency, and GNI is engaging as part of this group to work to improve government transparency practices, consistent with the FOC's commitment to: "Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance … while committing ourselves to do the same."[4]

We are concerned about the overly broad scope of UK lawful interception and communications data powers, as well as the marked absence of public consultation around significant policy and legal changes. Paired with the UK's standing and influence on the world stage, this approach is likely to be copied and it gives unintended justification in particular to governments who seek to limit human rights and this could undermine the effectiveness of the UK's efforts to advance freedom online. Other countries planning similar laws are already using the UK's position to validate their own legislative programmes in this area.[5] It is worth stressing the potential human rights abuses that such laws could create in those countries, including to UK citizens.

This review presents a rare opportunity to guide future governments on how to better balance the legitimate needs of law enforcement with international human rights standards, both in the formulation of policy and its execution.

We urge you to develop reform proposals for lawful interception and communications data that would serve as a worthy model for other countries to adopt, mindful that policy and legislation in the UK is often emulated by governments in the Commonwealth and around the world.

The changing global context

It is the duty of a government to protect its citizens and also to respect, protect, promote, and fulfil human rights. This includes ensuring that national laws, regulations, and policies are consistent with international human rights laws.[6]

---

[3] GNI Principles and Implementation Guidelines available at https://globalnetworkinitiative.org/corecommitments/index.php.

[4] Available at http://www.freedomonline.ee/foc---recommendations.

[5] ZDNet " Data retention is the way western nations are going: Brandis" July 16, 2014 available at http://www.zdnet.com/au/data-retention-is-the-way-western-nations-are-going-brandis- 7000031658.

[6] Guidance on these circumstances can be found in Articles 17 and 19 of the ICCPR. See also General Comment 16 of the Human Rights Committee; and UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, Frank La Rue, U.N. Doc A/HRC/23/40, April 17, 2014, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Finding the right approach is not easy, particularly in the global, complex, and constantly evolving ICT sector. At the same time, we note that threats, capabilities, and technologies are not the only factors that are evolving with respect to the interception of communications. Huge amounts of data are flowing across borders and being stored in multiple jurisdictions. For example, 100 hours of video are uploaded to YouTube every minute, double the rate from 2011.[7] Technological advancements mean that it is easier than ever to collect, analyse, and store communications data at scale, but also increasing the human rights risks in the event of the misuse of such practices.[8]

A 2014 BBC poll of 17 countries around the world found that 52% of citizens do not believe that "the internet is a safe place to express my opinions." In the UK, more than one in three respondents (38%) did not believe they were free from government surveillance.[9]

Meanwhile, public perceptions of the relationship between the government and private sector companies who often host their personal data have evolved considerably in recent years, particularly in the wake of the Edward Snowden disclosures. Beyond undermining user confidence in their freedom to express their views and maintain privacy, the extensive surveillance practices revealed in the last few years have done serious economic damage to the Internet and broader economy.[10]

Compounding these problems, governments around the world have sought to use the Snowden revelations to exert greater control over online communications in their territory and beyond. In some cases this includes mandating communications providers to store data locally, most recently in Russia.[11] In others, governments are asserting extraterritorial jurisdiction over data controlled abroad. At the international level, there are heated debates

---

[7] See YouTube statistics available at https://www.youtube.com/yt/press/statistics.html and http://youtube-global.blogspot.jp/2011/05/thank-youtube-community-for-two-big.html.

[8] Kevin Bankston and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones," Yale Law Journal, January 2014, available at http://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out--of--united-states-v-jones.

[9] BBC World Service Poll, 31 March 2014, available at http://downloads.bbc.co.uk/mediacentre/bbc-freedom-poll-2014.pdf.

[10] Danielle Kehl with Kevin Bankston and Robert Morgus, "Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom, and Cybersecurity," New America Foundation Open Technology Initiative, July 2014, available at http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf.

[11] See Moscow Times, "Russia Asks Facebook, Google, Twitter to Comply with Law on Data Storage," 26 September 2014, available at http://www.themoscowtimes.com/news/article/russia--demands-facebook-google-and-twitter- comply-with-law-on-data-storage/507852.html.

and the future of Internet governance, a topic that will next be on the agenda at the 2014 ITU Plenipotentiary Conference. In these debates, authoritarian regimes are seeking to exert a greater degree of control over the Internet.

A wide array of stakeholders have responded to government surveillance revelations by calling for reforms that would bring law enforcement powers and surveillance programs into alignment with international human rights standards. More than 400 civil society organizations, as well as academics and prominent individuals, and elected officials and political parties have endorsed the International Principles on the Application of Human Rights to Communications Surveillance.[12] Major Internet companies formed the Reform Government Surveillance Coalition and have issued their own principles to guide reform efforts.[13] Working together through GNI and in concert with other stakeholders, companies and civil society groups have advanced legislative reform proposals in the United States and succeeded in gaining greater ability to be transparent with the public about the national security requests they receive from the US government.[14]

UK legal framework

In September 2013, GNI wrote to the UK and other members of the Freedom Online Coalition (FOC), expressing concern that "the UK's communications surveillance practices, including both access to communications data as well as the interception of communications content, seriously threaten its reputation as a champion of Internet freedom and undermine your ability to advocate for other governments to support human rights online."[15]

The absence of constitutional constraints makes it particularly important that the UK reflect on how to define appropriate boundaries within law enforcement and surveillance powers should be defined and exercised. The current trend towards broadly worded, all--encompassing powers is particularly concerning.

Most problematic are practices that entail mass surveillance or bulk collection of user data. Mass interception or bulk collection of communications data threatens privacy and freedom of expression rights and undermines trust in the security of electronic communications services. This harm is caused both by direct bulk collection by governments, and by mandates that companies or other third

[12] International Principles on the Application of Human Rights to Communications Surveillance, available at https://en.necessaryandproportionate.org/text.

[13] See https://www.reformgovernmentsurveillance.com/.

[14] See Washington Post "US to allow companies to disclose more details on government requests for data" January 27, 2014 available at http://www.washingtonpost.com/business/technology/us--to-allow-companies-to-disclose-more-details-on-government-requests-for--data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html.

[15] GNI Letter to UK government, September 2013.

parties store data they would otherwise not retain in in order to facilitate government access.[16]

The UK government has consistently asserted, "All of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorized, necessary and proportionate."[17] However, it is difficult to square this statement with the disclosures of programs such as the unauthorised mass collection of webcam images from providers and other programs that are clearly disproportionate, of suspect necessity and for which the legal basis is, at best, unclear.[18]

The use of lawful interception and communications data in the UK is principally but not solely regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). But as the Interception of Communications Commissioner has himself stated, RIPA is "a difficult statute to understand."[19] Serious effort should be given to revising the complex and fragmented oversight regime, so concerned citizens can more easily understand these activities. This is particularly the case with regard to warrants issued under Section 8(4) of RIPA, where the Interception of Communications Commissioner's Office (IOCCO) has raised questions regarding the need for "the possibility of some structural or other consideration."[20]

The UK should halt the bulk collection of content and communications data from providers, and bring all data collection programmes under the auspices of an independent oversight regime.

Extraterritorial assertion of jurisdiction

GNI has observed a troubling legislative trend around the world in which requirements are placed on communications providers to respond to government requests for user data controlled outside that government's jurisdiction. Section 4 of DRIPA 2014 could provide unintended justification for such actions by other governments, including those that actively seek to limit freedom of expression and other human rights online. These provisions may encourage other governments to expand claims of jurisdiction without regard to

---

[16] As proposed in the 2012 Draft Communications Data Bill, although that bill was not formally introduced in Parliament.

[17] Marc Scott, "British Spy Agencies Assert Power to Intercept Web Traffic," New York Times, 16 June 2014, available at http://www.nytimes.com/2014/06/17/business/international/british-spy--agencies-said-to-assert-broad-power-to-intercept-web-traffic.html.

[18] It is not clear whether this and other GCHQ activities disclosed by Snowden are authorized under RIPA or other statutes. See the Vodafone Law Enforcement Disclosure Report: Legal Annexe for the UK legal powers governing real-time interception, disclosure of communications data, and national security and emergency powers, available at http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement_disclosure_report.pdf.

[19] The Rt Hon. Sir Anthony May, "2013 Annual Report of the Interception of Communications Commissioner," available at http://iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf, para1.6.

[20] Ibid., para 6.6.8.

the physical location of data centres, undermining the rights of UK citizens and the broader international framework for legal assistance.

Rather than asserting extraterritorial jurisdiction directly, the UK government should rely on other means of lawfully obtaining data from other jurisdictions, namely through mutual legal assistance treaties (MLATs). These treaties have not kept pace with the demand for communications and surveillance data, and are in most cases under resourced. The UK National Crime Agency has been a leading proponent of reforms to the MLAT process that would better address individual rights and law enforcement needs. GNI has commissioned a study on MLAT reforms that will be released later this year.

We recommend that the UK prioritize MLAT reforms as a more suitable approach to managing challenges around jurisdiction and cross---border data requests.

Transparency

GNI has urged greater transparency from the UK government regarding communications surveillance. Section 6 of DRIPA 2014 requires half-yearly reports from the Interception of Communications Commissioner's Office (IOCCO). However, an increase in the frequency of reporting alone will not improve the quality and effectiveness of these reports. The Home Office has assured GNI that "the government is wholly committed to ensuring that the use of communications data remains as transparent as possible."[21] Although the IOCCO 2014 report does represent a significant improvement from prior reports, with more information that is more clearly presented, there is much more that should urgently be considered to improve UK transparency.

There are both qualitative and quantitative aspects to transparency that need improvement. Qualitative disclosures include making publicly available the laws and legal interpretations authorizing electronic surveillance or content removal, among other measures listed below. Quantitative disclosures include the reporting of aggregate numbers of requests for user data or content removal, and the number of users impacted by these requests.

As well as making these disclosures themselves, the UK government should permit companies to issue analogous reports. The combination of government and company reporting can help the public understand the scope of surveillance. Under Section 19 of RIPA 2000, data relating to lawful interception warrants cannot be published, which significantly hampers public debate about the scope and scale of communications surveillance.[22]

The consequences of excessive secrecy surrounding data requests are now front- page news, with recent revelations that police have used RIPA to target

[21] Letter from Security Minister James Brokenshire to GNI, 11 November 2013.

[22] Vodafone Law Enforcement Disclosure Report.

journalists and reveal protected sources.[23] GNI welcomes the IOCCO inquiry into this matter, which attests to the importance of robust enforcement and transparency as well as the need for protections to ensure press freedom are incorporated into future reforms.[24]

We recommend that the UK government adopt the following transparency provisions regarding lawful interception and access to communications data:

- Publicly post information on the specific laws that authorize surveillance as well as official legal interpretations of the law, including executive orders, legal opinions that are relied on by executive officials, and court orders.

- Public disclosure of information about:
  - Which intelligence agencies/bodies are legally permitted to conduct surveillance;
  - The scope of the surveillance authorities of each of those entities;
  - The judicial, ministerial, other oversight mechanisms required for the authorization of each instance of surveillance;
  - The judicial, ministerial or independent oversight mechanisms that oversee the implementation of surveillance;
  - The mechanisms for redress that victims of unlawful surveillance may pursue; and
  - The scope of unlawful surveillance and remedial and disciplinary actions take.n

- Disclose to the victim of unlawful surveillance that unlawful surveillance has taken place as soon as practical, considering the needs of the specific pending investigation.

- Disclose aggregated information about the surveillance demands they make on companies including:
  - The number of surveillance demands;
  - The number of user accounts affected by those demands;
  - The specific legal authority for each of those demands; and
  - Whether the demand sought communications content or non-content or both, and how the authorities define these terms.

---

[23] Nick Kraven, "How police hacked Mail on Sunday phone," Mail on Sunday, 6 October 2014, available at http://www.dailymail.co.uk/news/article-2780809/How-police-hacked-Mail- Sunday-Officers-used-anti-terror-laws-seize-phone-records-identify-source-exposed-Chris-Huhne-s--speeding-points-fraud.html.

[24] "IOCCO Launches Inquiry into the use of RIPA powers to acquire communications data relating to confidential sources of journalists, 6 October 2014," available at http://www.iocco-uk.info/docs/IOCCO%20inquiry%20into%20use%20of%20comms%20data%20to%20identify%20journalistic%20sources.pdf.

- Permit companies to disclose, with the level of detail set out above, aggregated information on number of surveillance demands that they receive and how they respond to them on at least an annual basis.

- Permit companies to disclose technical requirements for surveillance that they are legally bound to install, implement, and comply with such as requirements to design lawful intercept capability into communications technology and to decrypt encrypted communications.

Consistent with the above recommendations, GNI believes that the declassification of an array of documents by the US government in the wake of the Snowden disclosures and in response to legal challenges by civil liberties organizations offers an instructive model for the UK to consider.[25]

Conclusion

The independent review of the legal framework for communications data and interception provides an opportunity for the UK government to rethink how it approaches policymaking at the intersection of national security and human rights concerns. **Building upon this call for evidence, we recommend a broad process of consultation including industry, civil society organizations, and other key stakeholders to aid in the development of policy options for public debate, informed by human rights impact assessments.** Both the process and the substance of UK policy and legislative review should ensure a rights-based approach worthy of adoption globally.

October 2014

[25] See http://icontherecord.tumblr.com/tagged/declassified for documents released by the US intelligence community following declassification review and in response to Freedom of Information Act requests.

Richard Greenhill

Need for new criminal offences and certainty in the law

Summary

Need for offences under DRIPA

1. The Data Retention and Investigatory Powers Act 2014 (DRIPA) lacks criminal sanctions for breaches by (on the one hand) public telecommunications operators (PTOs) who might refuse to retain data; or (on the other hand) by PTOs or third parties who might unlawfully disclose retained data.

2. Since even a single PTO might well possess retained metadata from hundreds of millions of communications involving tens of millions of individuals from the UK and throughout the world, unauthorised disclosure of data on just a single USB drive could have a catastrophic effect on the safety and well-being of millions of people, including those in fear of global organised crime and undemocratic states. Consequently, specific powers are needed to deter negligence and to punish determined wrongdoers.

Need for a bugging offence

3. Part 2 of the Regulation of Investigatory Powers Act 2000 (RIPA) regulates use of non- interception surveillance by public authorities, but fails to criminalise even wilful breaches. Surveillance by private bodies or individuals is left unregulated.

4. This has the perverse effect that unlawful interception is criminalised by part 1 of RIPA, whereas bugging similar face-to-face communications is not, in itself a criminal offence – even if it is conducted by third parties without notification and in the most private of places, such as the victim's home. The covert nature of bugging and the potential vulnerability of victims mean that civil law alone is wholly inadequate to deter or punish non-compliance.

Need to remove uncertainty in the RIPA saving provision

5. Section 80 of RIPA contains an unusual and sweeping saving provision, essentially providing that nothing in the Act implicitly repeals existing statutory or non-statutory investigatory powers. Potentially, public authorities may be making unexpected use of obscure laws or prerogatives. This prevents citizens from having confidence that they know all their rights. The ECHR requires certainty in the law, which section 80 undermines.

Data retention

6. Regulations 13(2)(*b*) and 15(11)(*b*) of the Data Retention and Investigatory Powers Regulations 2014 (SI 2014/2042), made under DRIPA, permit the Secretary of State to withhold reimbursement of expenses if a PTO or telecommunications service provider fails to co-operate with a data retention audit by the Information Commissioner. In addition, regulations 12(2) and 15(9) provide for enforcement by civil proceedings by the Secretary of State for an injunction or specific performance of a statutory duty if DRIPA is breached. Neither of these approaches is well-suited to a PTO which is determined not to co-operate.
7. More importantly for public confidence, DRIPA and the regulations fail to provide any direct sanction against PTOs or third parties unlawfully disclosing retained data.

8. Given the huge amount and sensitivity of retained data – relating to people from around the world, held in a relatively small number of locations – it is likely that data would be much sought after by undemocratic foreign states and other unscrupulous wealthy organisations and individuals.

9. Retrospective sanctioning of PTOs by withholding reimbursement for audit failures is therefore grossly inadequate as a deterrent or punishment. Further, the omission forces police and prosecutors to rely on general criminal offences when investigating malicious breaches or infiltration by third parties. Existing offences may be difficult to apply to the particular circumstances of bulk data retention and may lack proportionate punishments. The existence of specific offences would be likely to make PTOs and potential wrongdoers more mindful of the likelihood and consequences of major breaches.

Existing offences

10. Offences such as theft or computer misuse might apply. However, their terms and maximum punishments have not been considered by Parliament in relation to bulk data retention where a single abuse of trust could harm millions of individuals. Given the quantity of PTOs and the complexity of retaining (and periodically destroying) bulk data, DRIPA requires a large number of individuals in numerous private organisations to act with great care and to be incorruptible. The implications of this risk were not adequately addressed during the few days in which DRIPA was debated prior to its enactment.

Bugging

11. For want of a concise established legal term, this submission uses "bugging" to refer to covert sound or video recording of an individual by a local device, where the individual has a reasonable expectation of privacy.

12. Bugging, in itself, is not a crime.

13. This is in stark contrast to intercepted communications (criminalised by section 1 in part 1 of RIPA). So reading a postcard might be a RIPA section 1 offence, but videoing unsuspecting people in their own home might not be.

Inadequacy of existing laws

Data Protection Act 1998

14. The Data Protection Act 1998 (DPA) is indirectly a potential criminal deterrent to bugging. Section 55(1) makes it an offence to obtain or disclose data unlawfully, and subsection (5) similarly prohibits the sale of unlawfully obtained data. But this does not appear to prohibit creating data unlawfully in the first place. So someone making and hoarding surveillance recordings is not, on the face of it, committing an offence.

15. Sections 17 and 21 together create a criminal offence for failing to register under the DPA. But this does not cover bugging by a registered person nor does the administrative failure to register correspond clearly to the extreme invasion of privacy which may result from bugging. Conversely, a determined miscreant might register with no constraining effect.

16. In addition, all of the above DPA offences are limited by section 60(2) to punishment by a fine. There is no risk of imprisonment. So a malicious person who is wealthy or penniless may feel little deterrent for even the most serious of transgressions.

17. Section 77 of the Criminal Justice and Immigration Act 2008 permits the Secretary of State to amend the DPA so that a section 55 offence can alternatively be punishable by imprisonment for up to 2 years (which matches the existing maximum term for unlawful interception under RIPA section 1). However, this power has not yet been exercised.

Regulation of Investigatory Powers Act 2000

18. Part 1 of RIPA relates only to the interception and disclosure of communications.

19. Part 2 of RIPA covers bugging by public authorities but creates no criminal offences. It does not regulate private organisations or individuals, and there is uncertainty even as to how it regulates the increasing number of contracted-out services.

Criminal offences and regulation under other Acts

20. Part 3 of the *Police Act 1997* provides for oversight of authorities by the Surveillance Commissioners. But it creates no criminal offences. Moreover, section 92 provides that no authorisation "shall be unlawful if it is authorised" under part 3. In other words, part 3 is an enabling and oversight provision, not explicitly a prohibition.

21. The *Computer Misuse Act 1990* covers hacking into victims' computers, rather than wrongdoers using their own surveillance devices.

22. Section 13 of the *Theft Act 1968* covers abstracting electricity and has been used in a wide range of circumstances, but is inapt where a device is self-powered or connected to a perpetrator's nearby power supply.

23. The various *Wireless Telegraphy Acts* cover unauthorised radio transmissions and do not relate to bugging by local devices.

24. Section 2A of the *Protection from Harassment Act 1997* was inserted by section 111(1) of the Protection of Freedoms Act 2012 with effect from 25 November 2012. Notably, section 2A(3)(*g*) gives "watching or spying on a person" as an example of an act associated with stalking for the purposes of the offence. However, by subsection (1), section 2A prohibits stalking only if it also "amounts to harassment". So the offence is not suited to spying intended to remain unknown to the victim. And it would not cover spying on a broad range of people rather than harassing any one of them; or corporate espionage.

25. Chapter 1 of part 2 of the *Protection of Freedoms Act 2012* appoints the Surveillance Camera Commissioner and purports to cover "regulation of CCTV and other surveillance camera technology". However, the chapter creates no offences and section 33 provides that the "surveillance camera code does not of itself make [anyone] liable to criminal or civil proceedings". Only certain public bodies are required even to have regard to the code, though the Secretary of State has the power to extend the code to others. The code does not cover covert surveillance.

26. Section 67 of the *Sexual Offences Act 2003* criminalises "voyeurism" (including the associated use of recording equipment), but only "for the purpose of obtaining sexual gratification" and, by virtue of section 68, only if the acts observed for that purpose involve nudity, using a lavatory or intimate sexual behaviour. This would preclude prosecution if the purpose were not sexual (provable beyond reasonable doubt) or if gratification were sought without viewing such acts.

27. The *Official Secrets Acts* and related laws cover state security but do not protect private organisations or individuals.

Misconduct in Public Office

28. The common law offence of misconduct in public office is vaguely defined by case law but would, in principle, apply to public servants who seriously abuse surveillance powers. However, its ill-defined scope and its limitation to state employees make the offence inadequate for unlawful invasions of privacy which do not involve official corruption. The breadth of the offence also makes it poorly suited to deterring the unique intrusiveness of bugging.

General civil protections and human rights

29. Under the civil law, damages or injunctions may be obtainable for breaches of confidentiality or privacy. In particular, public authorities are liable for breaches of privacy under the Human Rights Act 1998 and Article 8 of the European Convention on Human Rights (ECHR).

30. But bugging is, by its nature, covert, so victims might well never become aware that they are entitled to damages – in clear contrast to typical civil wrongs such as nuisance or contractual breach. Confidential settlements may buy the silence of some victims, keeping others unaware that their rights have been (or will be) similarly breached. Unscrupulous defendants are unlikely to comply fully with disclosure orders in civil proceedings. Police and prosecutors are unable to investigate and conduct cases for solely civil breaches. More generally, public and private organisations may be unwilling or legally unable to assist witting or unwitting victims of civil breaches. In contrast, there is a compelling ethical duty to report and assist with the investigation of breaches which appear to be criminal.

Uncertainty in the law under RIPA general saving

31. In part 5 of RIPA, section 80 contains a broad "general saving for lawful conduct". It states that nothing in RIPA makes anything unlawful "which is not otherwise unlawful under this Act and would not be unlawful apart from this Act". This sweeping provision makes it unclear which, if any, common law, prerogative or pre-RIPA statutory investigatory powers remain in force in addition to those spelt out in RIPA itself. This catch-all has the potential to create needless uncertainty for anxious citizens and diligent public authorities.

32. The vagueness of the saving also subverts the requirement under Article 8(2) of the ECHR that any interference with privacy by a public authority must be conducted "in accordance with the law". Specifically, the European Court of Human Rights has held that the law must be publicly accessible to citizens; and the language of the law must be sufficiently clear to make interferences foreseeable. Though ECHR cases concerning RIPA have not raised section 80, its continued existence seems inimical to Article 8(2). If it has a practical effect, then the relevant saved powers should be listed and, if appropriate, codified. If section 80 has no practical effect, then it should be repealed.

Conclusion

33. Though the Investigatory Powers Review is focused on the regulation of public authorities, three particular anomalies in the law undermine effective regulation, deterrence of breaches and the protection of society:

(a) Serious breaches of DRIPA should specifically be criminal offences, with severe maximum penalties for the worst cases of unauthorised disclosure.

(b) Bugging should be a specific criminal offence, with exemptions for investigations conducted in accordance with RIPA part 2 or for a proportionate purpose or in the public interest. Public debate is needed as to the exact boundaries of such an offence, but widespread support for remote interception offences suggests there would be approval for criminalising grave invasions of privacy which result from unlawful bugging.

(c) The general saving provision in section 80 of RIPA should be repealed or replaced by a specific list of preserved powers.

October 2014

Guardian Media Group

Submission to ISC enquiry into privacy & security

Introduction

1. Guardian Media Group (GMG) is pleased to respond to the Intelligence & Security Committee's (ISC) enquiry into the balance between privacy and security. GMG is the publisher of the Guardian newspaper, associated Guardian applications and website, and a range of other businesses for whom digital technology is vital for its present and future economic prosperity.
2. GMG's future is wedded to the growth of the UK digital economy, and to the enabling power of the internet to access new markets across the globe. As we near the 25th anniversary of the British creation of the World Wide Web, it is important that the UK leads the long term debate about securing an open and secure internet in word and deed, to ensure that individuals and businesses can have faith, confidence and trust in the online world.
3. While the primary focus of debate about the Snowden revelations has been a binary debate between the competing public interests of privacy and security, the reporting of the Snowden files by the Guardian and many other newspapers across the world illuminate a range of other public interest considerations that the ISC should weigh in the round in order for this enquiry to have suitable credibility. These include the consequences of agency programmes that have:
    a. **Risked the integrity of the web itself** through the weakening of encryption protocols used by businesses and consumers through the insertion of backdoors[1];
    b. **Undermined legal privilege in commercial and criminal cases**[2] and put at risk the confidentiality of journalistic sources and material;
    c. **Risked the future of the digital economy,** with one Washington-based foundation predicting a potential economic loss to the US cloud computing industry alone of as much as $35 billion over the next 3 years through to 2016[3];

[1] Revealed: how US and UK spy agencies defeat internet privacy and security http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[2] Complaint filed over UK spying on Libyan torture victims' legal communications http://www.reprieve.org.uk/press/2013_10_14_PUB_UK_spying_libyan_torture_victims/
[3] http://www2.itif.org/2013-cloud-computing-costs.pdf

d. **Undermined the moral weight** of public statements made by UK and US leaders about the importance of an open internet[4];

e. **Made a mockery of the concept of Parliamentary sovereignty**, by circumventing the twice-stated will of Parliament to reject Government calls for the capability to bulk collect the digital communications of British citizens.

4. In weighing these public interests, GMG absolutely recognises that there are aspects of the workings of the intelligence agencies that must remain secret. GMG also recognizes the difficulty of debating the previously secret activities of organs of the State in public. However, as President Obama said last year *"What makes us different from other countries is not simply our ability to secure our nation… It's the way we do it, with open debate and democratic process."*[5]

5. In the absence of such political leadership in the UK, this enquiry represents both a huge opportunity, and a huge test for the ISC to demonstrate to the British public that it can balance arguments across the full range of public interests at play in this debate. Time after time in recent years, whether in relation to the rendition of UK citizens, or the torture of citizens in Libya[6], the ISC has failed to hold the UK intelligence services to account on behalf of Parliament and the British people. It is unsustainable that it should fall to journalists, courageous backbench MPs and NGOs to hold the intelligence agencies to account, especially – as this submission details later on – if the very programmes that form the centre of this debate potentially undermine the confidentially of journalistic sources and material.

6. Following the publication of the Snowden revelations, the contrast between the debate in the UK and the United States is stark. In the US there is a deep

[4] *"The WAN-IFRA membership is deeply concerned by the British authorities' treatment of the profession of journalism and its attempts to control the public debate.*
"The British government's actions have far reaching consequences across the globe -- particularly within the Commonwealth -- and any threats to the independence of journalism in Britain could be used by repressive regimes worldwide to justify their own controls over the press.
http://www.wan-ifra.org/press-releases/2014/01/15/global-press-freedoms-organisations-begin-press-freedom-mission-to-the-uni

[5] http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward-snowden-patriot/

[6] http://www.newstatesman.com/politics/2013/12/intelligence-and-security-committee-governments-white-washing-body-choice

and robust debate about the balance between privacy and security, leading to sweeping Presidential reforms. Contrast the findings of the Privacy and Civil Liberties Oversight Board, an independent liberties advocate in the executive branch, with the unchallenged assertions of the heads of UK intelligence services about the efficacy of these intelligence programmes in their first public appearance in front of the ISC on 7th November 2013.

7. In the United States we have seen the media, the general public, policy makers and the President address what is and will remain one of the most important challenges of our lifetimes – the limits of state power over our digital lives. The debate has been open, transparent and honest, most recently on 23rd January 2014 with devastating findings of agency overreach by the President's own Privacy Oversight Board[7]. This approach has led to wide-reaching Presidential reviews, a range of bi-partisan Acts in Congress, cases brought before the courts challenging the legality of the practices of the NSA, and a series of reforms announced by the White House. It is now time for the UK Parliament to reassert its control over agencies and programmes operating at the very edges of laws created for a different era.

8. In the remainder of this document, GMG outlines:

   a. Why RIPA 2000 is an inappropriate framework to govern intelligence agency activity in a radically-changed digital world;

   b. Why the distinction between 'content' and 'metadata' is artificial, raising questions about the lax oversight in relation to the capture and analysis of metadata;

   c. Concerns about the inadequate regulation of extraterritorial data transfers;

   d. Specific concerns about the inadequacy of the public oversight and transparency framework in which the agencies operate;

   e. The case for the use of intercept evidence in court;

   f. Concerns about the use of mass interception on privileged journalistic material.

[7] http://www.theguardian.com/world/2014/jan/23/nsa-barack-obama-phone-data-collection-illegal-privacy-board

Interception in a digital world

9. The argument made and lost by the previous Labour and, more recently, Coalition Government, that the law enforcement and the intelligence services in the UK need new powers in order to 'maintain the capability' of the State in a digital age falls down on two counts:

   a. First, far from maintaining the capabilities of the security services, the Intercept Modernisation Program, then through the Communications Capabilities Development Programme (CCDP) and the proposed Data Communications Bill, aimed to capture, store and analyse vast amounts of private communications on a scale that would have been inconceivable in a pre-digital age. Programmes like Tempora – revealed to the public and to the ISC in the Guardian – enable the intelligence services to intercept vast amounts of data stored or shared using modern electronic communications systems, by placing data interceptors on transatlantic internet cables.[8] The fact that the UK is a key landing point for transatlantic subsea cables enables the intelligence services to access a very substantial proportion of global internet traffic.

   b. Second, the importance of digital communications technology and platforms to the lives of consumers has increased dramatically between 2000 and 2014. In just one of the programmes identified in the Snowden files, GCHQ is estimated to handle in the region of 600 million "telephone events each day".[9] This is not to mention the enormous volume of personal information held on social networking sites such as Facebook by online retailers, banks and others.

10. The combination of the cheap electronic storage of vast amounts of citizen data with hugely powerful datamining and link analysis programmes provides intelligence agencies with huge insight into the behaviour of groups and individuals. Sophisticated computing can identify embedded patterns and relationships, including personal information, habits, and behaviour. Individual pieces of data that previously carried little potential to expose private information may now, through datamining and link analysis, reveal sensitive personal, privileged or professional information pertaining to individuals and organisations. This is of particular concern in the context of journalism, where the confidentiality of contacts and journalistic sources are of vital importance.

[8] The Guardian has reported that "by the summer of 2011, GCHQ had probes attached to more than 200 internet links, each carrying data at 10 gigabits a second" and that this mode of surveillance potentially gives GCHQ access to 21 petabytes of data a day. A petabyte is approximately 1000 terabytes (which is in turn 1000 gigabytes). This quantity of data is equivalent to sending all the information in all the books in the British Library 192 times every 24 hours, "GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications", The Guardian, 21 June 2013.

[9] *Ibid*

11. Following Parliament's refusal to pass either the Intercept Modernisation Programme or the Draft Communications Bill, these intelligence agency capabilities have been shoehorned within the existing provisions of RIPA 2000, raising huge questions about their legal basis as a consequence.

Section 8 (4) of RIPA 2000

12. A key problem with the present legislative framework for the interception and collation of data concerns the inadequate and outdated regulation of the collation of "external communications", which encompasses gargantuan quantities of personal, professional and privileged data pertaining to UK nationals and residents as well as businesses operating in the fields of commerce, law, media (including journalism) and industry. Section 8 (4) of RIPA 2000 removes the requirement, in respect of the interception of "external communications", that a warrant providing authorisation for interception must specify a particular person or "set of premises" to be made subject to interception. Moreover, as long as authorisation is provided by the Secretary of State, Section 8 (4) merely requires the warrant to provide the descriptions of "intercepted material the examination of which [the Secretary of State] considers necessary" in the interests of "national security", "preventing or detecting serious crime", or "safeguarding the economic well-being of the United Kingdom".[10]

[10] Section 8 (4), RIPA 2000.

13. As a result, "external communications",[11] defined as a "communication sent or received outside the British Islands" (which will include the huge range of data stored on servers located outside the United Kingdom) can be intercepted on a more imprecise basis than other communications. In practice, GMG understands from external legal counsel that Section 8 (4) warrants authorise the interception of generic and vaguely-described forms of material and are renewed on a six monthly basis (so are in place, in effect, indefinitely).

14. Parliament could not have envisaged either (i) the exponential growth in capacity for the collation and processing of information on a gargantuan scale; or (ii) crucially, the extent to which, through social networking and other online facilities, vast quantities of personal, privileged and professional data would be stored and communicated online. The legislative framework is therefore outdated.

15. Furthermore, from a legal perspective, it is very doubtful whether this scheme complies with the requirements of Article 8, ECtHR.[12] It is well-established that the collation and storage of information by State authorities on individuals amounts to an interference with the right to a private and family life which must satisfy the requirements of Article 8.[13] In particular any interference must be "in accordance with law" (in particular satisfy the need for legal certainty and foreseeability), and must manifest sufficient safeguards against arbitrariness and satisfy the criterion of proportionality. In relation to practices under Section 8 (4), key problems include:

    a. No meaningful assessment of proportionality of interference can be undertaken at the level of generality at which generic interception warrants are granted;

11 *See* Section 8 (5), RIPA 2000.

12 Note that *Kennedy v. the United Kingdom*, which found that aspects of the interception regime set out in RIPA 2000, was not concerned with the regime concerning "external communincations". *See Kennedy v. the United Kingdom* 52 EHRR 4 (2011).

13 This was confirmed recently by the Court of Appeal in *R. (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2013] 1 W.L.R. 3305. It is a position established by the ECtHR in a series of cases e.g. *Segerstedt-Wiberg v Sweden* (2006) 44 EHRR 14. In the context of the EU Charter of Fundamental Rights, see the recent decision of the Advocate General of the CJEU in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* Case C-293/12 finding that EU directive 2006/24/EC that requires telecoms and internet providers to store data on phone and email traffic for two years is a "serious interference" with citizens' right to privacy.

b. It appears that, in practice, permission for generic authorisation warrants are granted on a rolling basis and in place indefinitely;

c. As regards foreseeability and arbitrariness, the circumstances in which an individual or group's communications may be intercepted, retained and processed is wholly unclear. Indeed, the existence of the programmes had not even been formally acknowledged before the Guardian's reporting.

d. The degree of intrusion authorised through the generic warrants is considerable, justified by reference to broad, abstract notions of "national security", "the prevention of serious crime" or the economic welfare of the United Kingdom.

Reform required

16. GMG agrees with the proposal of the Parliamentary Joint Committee of Human Rights that "RIPA 2000 be amended to provide for judicial rather than ministerial authorisation of interceptions, or subsequent judicial authorisation, in urgent cases".[14] GMG submits that this approach should be applied both to the authorisation of communications internal to the United Kingdom and for "external communications".

17. The present system offers insufficient safeguards of independence in the authorisation process. Secretaries of State, who are responsible under RIPA for the issuing of sweeping, generic "certificates" for the interception of "external communications", are asked to authorise interception by agencies for which they are ultimately responsible. Government departments are often under enormous political pressure, whether from foreign governments for cooperation, from the public to respond decisively in the fight against terrorism and other serious crime, or to protect jobs and promote economic welfare. The risk that overbroad or intrusive authorisations may be granted in pursuit of these goals, influenced by these political pressures, is great. Politicians, much less ministers, can hardly be expected to be immune from

[14] Joint Committee on Human Rights, Counter-Terrorism and Human Rights: 28 Days, Intercept and Post Charge Questioning, (HL 157/HC 394), 30 July 2007, at 161.

the pressure of politics and public opinion. Real concerns therefore exist as regards whether authorisation by the SSHD provides sufficient independence and serves as an effective safeguard for privacy.

18. This is born out in practice. Although figures are not publicly available it has been acknowledged by successive Interception Commissioners that the refusal of a warrant by a Secretary of State "is rare".[15] This has, it appears, been the case for many years. Real doubts therefore exist as to whether the authorisation process serves to provide meaningful scrutiny of requests.

19. Judges or, at the very least, persons independent of political pressures offer the best safeguards of independence and impartiality. This is all the more important given that interception decisions are necessarily made in secret when affected persons have no opportunity to seek to protect their own interests. As the ECtHR held in *Klass v. Germany*:

a. *The rule of law implies … that an interference by executive authorities with an individual's rights should be subject to 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.*[16]

20. Furthermore, a system of judicial authorisation is eminently workable — indeed, is perhaps preferable on grounds of efficiency to the system presently in place. In this regard, the following points should be noted:

   a. Precisely this system operates successfully in many European states and in many democracies in other regions of the world;[17]

   b. High Court judges are very experienced in dealing with very complex matters, on an urgent or very urgent basis, and deal with requests for urgent relief often within a matter of hours if necessary (including out of hours and at weekends or on public holidays);

15 *See e.g.* Report of the Interception of Communications Commissioner for 2003, July 2004, at 8 and, to similar effect, Report of the Interception of Communications Commissioner for 2009, at 2.3; and Report of the Interception of Communications Commissioner for 2010, at 2.4.

16 *Klass v. Germany*, 2 E.H.R.R. 214 (1980). *See also Popescu v. Romania* (No. 2), Merits, 26 April 2007, Application No. 71525/01 at 70-73 and *Lordachi v. Romania*, 10 February 2009, 25198/02, at 40, where the Court held "the body issuing the authorisations for interception should be independent … and there must be judicial control or control by an independent body over the issuing body's activity".

17 See *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime*, United Nations Office of Drugs and Crime, available at: http://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

c. A High Court judge is likely, by virtue of his or her professional experience and background, to be better equipped to deal with the issues at stake (in particular weighing up the different legal interests) speedily and effectively than a Secretary of State, relying on the assistance and advice of his or her officials. The Secretary of State may well consider the matter diligently but has no necessary experience of acting in a judicial or quasi-judicial capacity, weighing different, often competing legal interests and considering matters such as the proportionality of interference;

d. Needless to say, a judicial authorisation process could be conducted *ex parte* and need not involve court proceedings or the formality of such proceedings.

21. In short, a process of prior judicial, rather than executive authorisation, would undoubtedly be effective in practice. It would offer greater guarantees for the rule of law, provide more independence and offer much greater reassurance that the legal framework in place, including the public's right to privacy, is respected.

The significance of Metadata

22. As a recent Guardian infographic demonstrates, the volume and variety of insight that metadata[18] generated by commonly-used digital services is significant. The privacy impact of collecting all communications metadata about a person or organisation over time (and aggregating and link analysing this data) is often vastly greater than the impact of collecting specific content data about a single person, group or organisation. There is no sufficient justification for the less rigorous and less independent regulatory regime applied in the context of metadata than that in relation to content.

23. Interception of content is authorised by the Secretary of State for three or six months (depending on the purpose) by a warrant specifying an individual or premises under Part I Chapter 1 of the Regulation of Investigatory Powers

[18] Metadata describes the characteristics of information or a communication, other than its content.

Act 2000. Interception of "communications data"[19] however, is regulated by the less rigorous regime set out in Part I Chapter 2 of RIPA.

a. First, the grounds on which communications data may be intercepted are much more expansive than those relating to content, including public safety, public health as well as the economic well-being of the UK, national security or the prevention and detention of crime (not just serious crime).[20]

b. Second, crucially, rather than authorisation being required by the Secretary of State,[21] a very wide range of "designated officials" in many different government departments and agencies may authorise persons in their agency to undertake the interception of metadata (in effect, a system of self-authorisation by various departments and agencies).[22]

24. The notion, oft repeated by Ministers and security officials, that metadata is less intrusive or meaningful than content is based on the discredited idea that metadata merely reveals matters such as the timings of particular emails or the location of computers used. Using new "dataveillance" and information synthesis technology, the collation of metadata now enables the exploitation of metadata in ways unimaginable at the time RIPA 2000 was enacted by Parliament, giving rise to substantial concerns about the collation of very sensitive, personal, professional or privileged information about individuals, groups, political parties, NGOs, media organisations, journalistic networks and their sources, lawyers and their clients, to give just a few examples.

Reform required

25. Where metadata is collated and exploited using information synthesis techniques, given that it poses as great a risk to individual privacy as content interception, it must be subject to the same regulatory regime, including

19 "Communications data" is defined, *inter alia*, as "any information which includes none of the contents of a communication [...] and is about the use made by any person–(i) of any postal service or telecommunications service; or (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system". It is therefore to be distinguished from the content of communications.

20 Section 22 (2), RIPA 2000.

21 Section 5 (1), RIPA 2000.

22 Section 22 (3), RIPA 2000.

appropriate independent authorisation. The present system for the authorisation of the interception of metadata by numerous "designated persons"[23] who work for the organisations which seek to intercept such data is unsustainable.

Insufficient Regulation of Extraterritorial Data Transfer

26. The present regulatory system fails to provide sufficient protection in respect of the growth of the extraterritorial transfer of collated data, again a phenomenon the nature and scale of which was not contemplated at the time RIPA 2000 was enacted. A number of points are important in this regard.

    a. First, the powers of the NSA and other US agencies to intercept communications data of non-US persons outside the United States (including UK residents) are considerable and subject to few safeguards. The power is set out in Section 1881 (a) of the US Foreign Intelligence and Surveillance Act 1978 and permits "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information".[24] There is no requirement that the surveillance need be proportionate, nor even that it be necessary to protect specific interests such as national security. The US National Security Agency, it is understood, has direct access to data collected through the Tempora system[25]. In consequence it may, under US law, use such data in circumstances or in a manner that would not satisfy the requirements of domestic UK law or the European Convention on Human Rights (particularly where such data

23 *See* Section 22 RIPA 2000.

24 The definition of "foreign intelligence information" is set out in s 1801. It is very broad. Pursuant to section 1801(e) "foreign intelligence information" includes "information with respect to a foreign power or foreign territory that relates to ... the conduct of the foreign affairs of the United States." The term "foreign power" is defined in section 1801(a) to include not only foreign governments or entities directed or controlled by foreign governments, but also pursuant to section 1801(a)(5) "a foreign-based political organisation, not substantially composed of United States persons." Foreign-intelligence information thus covers information with respect to any foreign-based political organisation or government that relates to the foreign affairs of the US. It would thus, for example, include the contents of private and lawful discussions by those who are members of, or are communicating with, political organisations or governments that in any way relates to US foreign policy. GCHQ has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process cast streams of sensitive personal information which it is sharing with the NSA in the United States. GCHQ taps fibre-optic cables for secret access to world's communications

concerns persons who are not US nationals or resident in the United States).

b. Second, limits on the use of data transferred to the United States are not publicly disclosed but are contained in the provisions of confidential agreements concluded between the United States and the United Kingdom. The United Kingdom is under an obligation not merely to refrain itself from arbitrary interference with the right to private and family life through the interception, retention and/or use of private information but is also, by virtue of the settled case law of the ECtHR, under a positive obligation to protect the right to private and family life from arbitrary interference by others. In *KU v. Finland*,[26] for instance, the ECtHR found violation where the State had failed to take "practical and effective" measures to protect the applicant's private life.[27] Given the scale of data collected through programmes like Tempora and the extent to which such data is transferred or made available to United States agencies, it is open to serious doubt whether the transfer and/or access is, given the limited safeguards in place, legal under United States law. These concerns are heightened given that the statute code of practice, prepared pursuant to Section 71, RIPA 2000, *Acquisition and Disclosure of Communications Data: Code of Practice*, expressly envisages situations where data is disclosed to other states "even though that country does not have adequate safeguards in place to protect the data".[28] Again, it is very doubtful whether such a practice is compatible with the requirements of Article 8, ECtHR.

Reform required

27. Under RIPA 2000 much depends on whether a communication may be described as an "external communication".[29] Crucially, where a communication is "external", a special

26 *See e.g. KU v. Finland* 48 EHRR 52 (2009), at 42.

27 *Ibid*. at 49.

28 7.21, *Acquisition and Disclosure of Communications Data: Code of Practice.*

29 "External Communication" is defined in Section 20 RIPA as "a communication sent or received outside the British Islands". "Communication" is, in turn, defined in Section 81 (1) of RIPA as "(a) … anything transmitted

form of interception authorisation may be granted (a Section 8 (4) Certificate). This certificate, issued by the Secretary of State, need not specify a particular "set of premises" or "person" to be targeted (as is required in respect of the interception of other forms of content communication under RIPA 2000). A huge proportion of information stored or shared on the internet may be treated as "external" and therefore subject to this less rigorous regime, given that a great deal of information or data will be stored on servers outside the United Kingdom.[30]

28. Section 8 (4) certificates have, in practice, provided almost no check on the interception of all manner of external communication in recent years. In practice, the ten or so generic warrants which appear to be in place authorise the interception of an enormously broad range of generically described information, permitting interception on an almost blanket basis. Much greater precision in the certification process is required (not least to comply, it is submitted, with Article 8, ECtHR). Given the clear failure of the certification process to perform its function of providing precision and a safeguard against overbroad data interception, the level of precision required of a certificate should be legislatively prescribed.

29. It is accepted that there may be a justification, in certain limited circumstances, for large-scale surveillance in certain aspects of foreign relations. The intelligence services may, for instance, quite properly seek to engage in surveillance of certain oppressive foreign governments or criminal or terrorist organisations. Blanket surveillance of this nature should, however, be strictly scrutinised and authorised by way of specific warrants, identifying the foreign governments, foreign government entities, groups, organisations persons or entities targeted, to enable a meaningful consideration of the proportionality of interception.

30. In short, alongside the existing safeguards to the certification process set out in Section 16 RIPA 2000, more precise requirements as to the level of detail

by means of a postal service; (b) anything comprising speech, music, sounds, visual images or data of any description; and (c) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus".

30 Note, however, that Section 16(1) and (2) RIPA 2000 provide that an interception warrant in respect of "external communications" may only be "referable to an individual" in the UK or "have as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him" if the Secretary of State certifies that this is necessary.

contained in a Section 8 (4) certificate should be specified in primary legislation. These requirements should bring to an end the practice of issuing generic warrants, at a very high level of abstraction, obviating meaningful or careful consideration of the proportionality and propriety of data interception.

Inadequate Public Oversight & Transparency

31. Present levels of public oversight and transparency are wholly inadequate. Through recent debates in Parliament it is clear that members of the ISC [31], and senior members of the Joint Committee that examined the Draft Data Communications Bill[32], were unaware of the existence of agency programmes reported by the Guardian.

32. Informed public debate about the many public interests involved in the interception of private information by the State should not be dependent on investigative journalism or whistleblowers. Available official guidance gives a wholly inadequate picture of the circumstances in which interception may take place.[33] Parliamentary debate, and the public more broadly, should be informed, at the very least, of the general nature of programmes in place and how such programmes are regulated in order to:

    a. **Protect legal accountability:** So that, if necessary, the question of whether a programme is lawful can be tested before the Courts, which is fundamental to the Rule of Law;

    b. **Protect against the arbitrary use of surveillance power:** By ensuring that categories of individuals, groups and organisations can understand the circumstances in which they may lawfully be made subject to the interception of data. Again this is fundamental to the Rule of Law;

31 http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm

32 http://www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance

33 See *Interception of Communications Code of Practice*, Seventh Impression 2007 and the *Acquisition and Disclosure of Communications Data Code of Practice*, First Impression 2007. It is entirely unclear from either of these documents that mass scale data interception has been authorised and is occurring. Indeed, the nature and scale of interception which is occurring is hard to reconcile with the statements of principle in the Codes of Practice. For instance, the Communications Data Code of Practice States that data interception will occur only when "necessary", "proportionate" and, "in accordance with law" (See 2.1, *Acquisition and Disclosure of Communications Data Code of Practice*).

c. **Ensure political and democratic accountability (and, if necessary, reform):** Given the ever-present speed of technological change in this area, the need for regulatory reform must be kept under continual review, which occurs in the context of a properly-informed public debate.

33. Without a properly-informed public debate, in which the nature of surveillance activities carried out are understood and the efficacy and propriety of the surveillance framework is the subject of continual review, the risk that the regulatory framework will become outmoded once more and that disproportionate surveillance methodologies will develop once again is considerable.

34. Given the fact that the ISC is the only Parliamentary Committee with any standing to hold the intelligence agencies to account, it is essential that through this enquiry, the public can be assured that the ISC is able has the powers, capabilities and resources to scrutinise the agencies activities. For example:

a. Following annual evidence sessions, and sessions in relation to the draft Data Communications Bill, is the ISC satisfied it was provided with sufficient information about existing capabilities and programmes?

b. Does the ISC have adequate resources and sufficient time to scrutinise the agencies' operations across the vast terrain it now roams on our behalf?

c. Are new powers to request any document it wishes from the security services enough to hold the agencies to account in the absence of the broader context in which to analyse their significance?

d. Do Members understand the extraordinarily complex and ever-evolving technology involved?

e. Does the Committee have enough external assistance from technical experts that have not worked for the agencies or their contractors?

f. Even after the reforms of the Justice and Security Act, is membership of the Committee sufficiently independent of Government?

g. Is it appropriate that Committee Members encumbered by decisions taken whilst a Minister with responsibility for agency activities should sit as Members of the ISC?

35. Alongside questions about oversight provided by the ISC, the ISC enquiry should consider the case for reform of the Investigatory Powers Tribunal (IPT). On the basis of information supplied by HM Courts Services, between 2001 and 2011 only 0.5 per cent of complaints were successful (6 cases out of 1,115). That is much less than figures for the same period before other tribunals and with no obvious reason why complaints made in a context marked by secrecy of decision-making would be substantially less meritorious.[34] Real concerns therefore exist as to whether the IPT provides an effective remedy in respect of unlawful interception. A number of substantial problems arise in respect of the IPT, its rules of procedure and, more generally, the fairness with which it operates:

a. First, the degree of secrecy surrounding IPT proceedings.[35] In the recent Supreme Court case of *Bank Mellat v. Her Majesty's Treasury* (No. 1) [2013] UKSC 38, the Court reaffirmed that "[t]he idea of a court hearing evidence or argument in private is contrary to the principle of open justice, which is fundamental to the dispensation of justice in a modern, democratic society". An almost blanket rule of secrecy, such as that applied by the IPT, is inconsistent with the fundamental principle of open justice and undermines public confidence in the operation of the tribunal.

b. Second, Section 67 (8) of RIPA 2000 provides an ouster of the jurisdiction of the High Court or, indeed, any other court to hear challenges to the decisions of the IPT.[36] The IPT cannot be assumed to be immune from errors of law or failures in fair

34 This compares to a success rate, in the same period of, for instance, 41% before the Immigration and Asylum Tribunal, 44% before the Criminal Injuries Compensation Tribunal, and 35 % in relation to tribunal cases concerning social security and child support. See *Freedom From Suspicion: Surveillance Reform for a Digital Age*, Justice October 2011.

35 Rule 9 (6), Investigatory Powers Tribunal Rules 2000. In *Kennedy v. G.C.H.Q* IPT/01/62, the IPT held that this provision, requiring all proceedings to be held in secret, was ultra vires. The rule, however, has not been amended and, in practice, hearings often proceed, even on matters of directions, without a claimant being notified of the hearing or provided opportunity to make submissions. All other rules were upheld by the IPT in Kennedy.

36 Section 67(8) of RIPA 2000 provides: "[e]xcept to such extent as the Secretary of State may by order otherwise provide, determinations, awards, orders and other decisions of the Tribunal (including decisions as to whether they have jurisdiction) shall not be subject to appeal or be liable to be questioned in any court."

procedure any more than another court. But this provision purports to prevent any such failure being challenged, which, in the event of a failure of fair procedure, likely violates Article 6, ECtHR.[37] This is all the more concerning since, under its rules, the tribunal cannot inform a party that a hearing has even been held (even on a matter such as directions) to enable submissions, even simply on issues of open justice or matters concerning the administration of a case, without the consent of the other party,[38] and a hearing will rarely be held *inter partes*. The scope for uncorrected errors of fact and law is therefore great.

Reform required

36. The efficacy of reforms made as a result of the passing of the Justice and Security Act (JSA) to strengthen the independence and resourcing of the ISC will take time to prove. However, in light of revelations that Members of the ISC were unaware of crucial agency programmes, calls made by Opposition Ministers during debates on the JSA that the ISC should become a full Select Committee of the House of Commons merit further consideration – not least because of the greater protection offered to witnesses and the potential penalties for misleading evidence provided to Select Committees.
37. There are substantial concerns regarding the fairness and efficacy of proceedings before the IPT and, given the statistics cited earlier, whether it provides an effective check on disproportionate or unlawful surveillance practices such as those reported by the Guardian. Fundamental revision of aspects of the IPT's operation is therefore required.

The use of intercept evidence in court

38. The UK is one of the very few countries which completely prohibits the use of intercept evidence in civil or criminal proceedings. GMG supports the view of

37 See e.g. *Kingsley v. the United Kingdom*, 35 EHRR 177 (2002).

38 IPT Rules 6 (2) - (4).

the *Privy Council Review Intercept as Evidence 2008*[39] that this prohibition should end.

39. Section 17 (1), RIPA provides that "no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of, or in connection with, any legal proceedings or Inquiries Act proceedings which (in any manner)– (a) discloses [...] any of the contents of an intercepted communication or any related communications data; or (b) tends ... to suggest that [interception had occurred or that a warrant for interception had been issued].

40. Most other countries regularly use intercept evidence in open court without any consequent loss of intercept capability, including other common law jurisdictions with similar criminal procedures and disclosure obligations to those which exist in the United Kingdom.[40] As the Prime Minister noted in a debate on the matter while in opposition in 2008, "'...*The Australian example, in particular, provides a number of interesting ideas for how the UK could attempt to derive benefit from intercept as evidence, whilst not unacceptably increasing the risk of disclosure to intelligence agencies and their sensitive capabilities and techniques.*"'[41].

Reform required

41. GMG understands there is broad Parliamentary consensus on the need to use intercept evidence in court[42], and urges the Government to look again at how the prohibition set out in Section 17 (1) RIPA be ended.

39 *See Privy Council Review Intercept as Evidence : Report to the Prime Minister and Home Secretary*, 2008, p. 31 Cm 7324.

40 See Privy Council Review Intercept as Evidence : Report to the Prime Minister and Home Secretary, 2008, p. 31 Cm 7324.

41 http://toryspeeches.files.wordpress.com/2013/11/david-cameron-statement-on-the-use-of-intercept-evidence.pdf

42 http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140121/debtext/140121-0003.htm#140121-0003.htm_spnew86

Mass Interception and Privileged Journalistic Material

42. As outlined above, GMG is especially concerned about the lack of safeguards in place to prevent the mass interception and collation of data by the intelligence services undermining privileged journalistic material and the confidentiality of journalistic sources. The security of such material is absolutely vital to the journalistic function in a democratic society, including journalism which seeks to hold the State and its institutions (including the intelligence services) to account. As Lord Woolf held in *Ashworth Hospital Authority v MGN Ltd* [2002] UKHL 29 [at 61]:

> *[I]nformation 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.*

43. It is well established in the jurisprudence of the ECtHR 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" (*Goodwin v. the United Kingdom* (1996) 22 E.H.R.R. 123, [at 39]).

44. Although the protection of journalistic sources is not absolute, it can only be abrogated where justified by "overriding requirement in the public interest" (a high threshold), with any restrictions subject to strict scrutiny by the Courts (*Goodwin v. the United Kingdom* (1996) 22 E.H.R.R. 123, [at 39-40]. GMG believes that a fundamental safeguard, in this context, is that the circumstances in which the confidentiality of journalistic material has been contravened must be "in accordance with law", meaning that the nature of any restriction must be clear, accessible and foreseeable.

Reform required

45. The mass interception of data and communications will *inevitably* result in journalistic material being intercepted and collated. However, whether there are presently any guidelines or safeguards in place as regards the handling of such material or its dissemination within government agencies (much less whether such safeguards are sufficient and lawful) is wholly unclear. In the absence of the publication of clear guidance and rules regulating and restricting the interception of journalistic material, particularly as regards the interception of "external communications", such a process can neither comply with the rule of law nor satisfy the requirement of legality under Article 10, ECtHR. At the very least, rigorous safeguards, which are clear and accessible to the public, are required.

February 2014