LIBERTY80

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's submission to the Reviewer of Terrorism's Investigatory Powers Review

November 2014

About Liberty

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

Liberty Policy

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

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

Contact

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

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

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

Introduction

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

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

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

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

The human right to respect for privacy

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

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

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

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

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

Consistent provision of safeguards

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

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

distinction between the two forms of information. In a recent ruling, which the US Government is appealing, a US District of Colombia judge extended the protection of the fourth amendment to communications data, stating:

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

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

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

---

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

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

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

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

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

Targeted surveillance instead of mass interception and communications data retention

Interception warrants

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

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

[8] Section 2 RIPA.

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

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

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

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

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

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

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

[11] Witness statement of Charles Blandford Farr on behalf of the Respondents in Case No IPT/13/194/CH, 16 May 2014, available at: https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf.

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

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

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

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

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

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

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

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

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

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

Communications data

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

---

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

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

[17] See footnote 8.

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

---

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

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

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

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

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

[26] Protecting the Public in a Communications Data in a Changing Environment, Home Office, April 2009, page 19, available at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/27_04_09communicationsconsultation.pdf.
[27] Report of the Joint Committee on the Draft Communications Data Bill, November 2012, para 230-1.

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

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

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

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

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

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

Establishment of a lawful and transparent framework for surveillance information sharing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

New requirement for prior judicial authorisation

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

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

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

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

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

---

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

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

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

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

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

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

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

Narrowing of purposes for which surveillance can be conducted

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

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

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

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

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

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

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

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

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

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

Redress for individuals subject to unlawful surveillance

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

Disclosure

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

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

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

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

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

---

[48] Liberty, Regulation of Investigatory Powers Bill: second reading briefing, House of Lords, May 2000, page 3, available at: http://www.liberty-human-rights.org.uk/pdfs/policy00/may-2000-ripa.pdf

[49] *Weber and Saravia v Germany*, 2006, application 54934/2000, paragraph 135.

Investigatory Powers Tribunal

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

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

Democratic oversight

Legislative scrutiny

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

Intelligence and Security Committee

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

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

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

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

The Intelligence Commissioners

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

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

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

56. In its recent report on counter-terrorism, the Home Affairs Select Committee expressed concern that the Interception of Communications Commissioner inspects only between 5-10% of applications made each year and the Intelligence Services Commissioner had examined only 8.5% of warrants. The Commissioner posts are only part time, which may account for the fact that so few investigations are conducted, but it remains the case that these are tiny proportions and conducting investigations into this amount of work offers no guarantee as to the health of the system in general.

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

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

Conclusion

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

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

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

Sara Ogilvie
Isabella Sankey