LIBERTY80

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's evidence to the Intelligence and Security Committee's inquiry into Privacy and Security

February 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 is pleased to have the opportunity to respond to the ISC's inquiry into privacy and security. The inquiry relates to public concern over the content of documents leaked by United States National Security Agency (NSA) contractor, Edward Snowden, in June 2013. The disclosures concerned US and UK Government surveillance programs, which allow access to vast swathes of private communications content and metadata held by communications providers.[1] The disclosures also detail the extent to which Governments have worked with communications providers to build 'back doors' into encryption software.[2]

2. The two most significant disclosures concern the 'Prism' and 'Tempora' programs. Prism is a mass electronic surveillance access and data mining program operated by the NSA since 2007 to collect 'foreign intelligence' information. The US Government has accepted the existence of Prism and the UK Government has followed suit. The UK has also accepted that it has been in receipt of data from Prism via its intelligence data-sharing relationship with the US. Tempora is described as "*a GCHQ program to create a large-scale 'internet buffer' storing internet content for three days and metadata for up to 30 days*"[3]. It is believed to have been operational for approximately two years and involves the tapping of more than 200 fibre optic cables. According to the leaked NSA documents GCHQ was handling 600 million telephone events via Tempora each day in 2012. The Guardian has also reported that GCHQ officials gave NSA officials access to material obtained by Tempora. The UK Government has adopted a neither confirm nor deny policy (NCND) in relation to Tempora.

3. Liberty does 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 the same aim. We also understand and accept the need for secrecy concerning operational capabilities and techniques to ensure that lawful surveillance is operationally effective. We don't therefore seek confirmation about the existence of Tempora or the agencies' surveillance techniques and capabilities. However the authorities' response to the leaks to date has been deficient -

[1] As reported in *The Guardian* and the *Washington Post* on 6 June 2013.
[2] *The Guardian,* 12 July 2013.
[3] *The Guardian,* 21 June 2013.

amounting to repeated ministerial statements that the UK has a strong legal and oversight framework for the work of the security agencies.[4] This is in stark contrast to the US response which has seen President Obama establish a review of surveillance law and practice and announce a number of reforms earlier this year.[5] Given public and international concern over the practices of GCHQ, the UK Government now needs to urgently engage with the many questions that surround the application of relevant domestic law and make important legislative reforms where necessary.

4. Liberty has lodged a claim against GCHQ, SIS and the Security Service in the Investigatory Powers Tribunal pursuant to section 7(1)(a) of the *Human Rights Act 1998* (HRA) on the basis that the respondents have interfered with the private communications of Liberty staff contrary to their rights under Articles 8 and 10 of the European Convention on Human Rights (ECHR). As well examining and resolving our substantive claim we hope that a public determination of the legal issues raised will shed some light on the legal framework.

5. Against this background, Liberty welcomes the ISC's gesture to inquire into privacy and security and consult civil society. In the spirit of constructive engagement, our submission responds to three specific questions posed by the Committee. However, Liberty has lost confidence in this Committee's ability to provide effective oversight of the security agencies. Despite some limited reforms in the *Justice & Security Act 2013*, the Committee is inadequately staffed and funded and does not have sufficient technical expertise. Of equal concern, public statements by Committee members reveal a somewhat unquestioning attitude towards the work of the security agencies. The Committee's annual reports consistently fail to critically analyse the agencies' claims and its recommendations do not seek to hold the agencies' to account but rather 'do the agencies' bidding' on matters as varied as funding and the creation of closed courts. In consequence, Liberty regards the ISC more as a spokesperson for the agencies than a credible oversight body. We do not consider it able to conduct a neutral inquiry into the laws that regulate their conduct.

[4] See Foreign Secretary's Statement to the House of Commons, 10 June 2013, Hansard Column 31.
[5] See Remarks by the President on Review of Signals Intelligence, 17 January 2014, available at: http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

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

How does this differ for internet communications when compared to other forms of surveillance, such as CCTV? To what extent is it necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security? 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)?

6. The notion of an individual right to privacy vs collective right to security is misguided. Everyone, by reason of their humanity deserves respect for private life *and* the protection of their security. Given the importance of privacy and dignity to democratic society, there is just as much a collective right to privacy as a collective right to security. Just as the two objectives are not diametrically opposed, they also don't stand in isolation.

7. Human rights have historically been understood as intrinsically linked and indivisible. Where privacy is breached other rights may necessarily be breached too, including the right to security. The availability of classified GCHQ documents to 850000 security contractors (as revealed by the Snowden leaks) demonstrates how the stockpiling of personal information has the potential to undermine security. Similarly, Abdel Hakim Belhaj's interim relief application in the IPT requesting that the security services undertake not to intercept and read private correspondence with his legal team demonstrates how privacy breaches can undermine the right to fair trial. A free press and the right to free speech are also partially dependent on respect for privacy. If someone believes that their innocent communications are being monitored, this will affect what they say and how they behave. In the case of a journalist or newspaper it will affect their ability to obtain information, protect sources and therefore publish in the public interest. In the most extreme example of the way in which human rights are co-dependent, a privacy infringement that allows sensitive locational information to be disclosed to a State engaged in extrajudicial killing or rendition and torture may result in an individual being unlawfully killed, fatally undermining their personal security.

8. The question considers the difference between CCTV surveillance and surveillance of internet communications. It is hard to generalise about CCTV

systems. CCTV can include privately owned cameras, local authority cameras covertly installed cameras and ANPR. Traditionally a distinction has been drawn between targeted surveillance and general CCTV surveillance; also between covert and open surveillance. A local authority CCTV camera looks at a public location and captures all passers-by rather than targeting a particular individual. It therefore represents less of an interference with privacy and so does not have to be justified with the same rigour as a specific request for targeted communications data or interception. Many CCTV cameras are also overt[6] thereby representing less of an interference than covert targeted surveillance as notification can allow an individual to take steps to avoid surveillance. Lastly while CCTV can - depending on the images caught – reveal highly personal and sensitive information (eg. someone's attempt to commit suicide) the substantive interference that can result from targeted surveillance is generally considered greater - interception, bugging, human covert surveillance and acquisition of communications data can reveal deeply personal information about someone's thoughts, views, thoughts, relationships, sexuality, politics.

9. Private and home life have an important tradition in Britain. While for many years it was not given the legislative expression that the right attracted elsewhere in the world (eg US, Europe) Article 8 of the ECHR as incorporated into domestic law by the HRA now protects right to respect for private and family life, home and correspondence. Crucially it is a qualified right, which can be interfered with 'in accordance with law' to pursue a number of legitimate public policy aims and where necessary and proportionate in a democratic society. Its limited nature recognises that at times there are tensions between the exercise of rights between individuals and within wider society. Proportionality requires that if there is a less intrusive way of achieving the same aim then the alternative must be used.

10. It is neither necessary nor proportionate in a democratic society to collect, monitor or process innocent communications in order to find those that threaten our security. Indeed this is why Britain – as opposed to totalitarian countries - has traditionally rejected this model. To take an example, the British postal service has never been required to intercept or store every letter or parcel it handles nor to make a note of the sender addressee and the time it was posted just in case the content or record of the package may in future be useful to the police or the security services.

[6] Although covert cameras can be installed under section 32 RIPA or inside property under Part III Police Act 1997 and section 5 ISA.

This important principle remains regardless of the mode of communication. Just because new ways of communicating electronically have made surveillance of innocents less expensive and burdensome than it may have been in the past, does not mean it is in society's interest to allow it.

11. As well as the harm to democracy and freedom, the lazy assumption that collection and retention of ever greater data troves reaps security benefits is 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 needed to disrupt terrorist plots "*could readily have been obtained in a timely manner using conventional court orders*".[7] 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*". [8] The study concluded that traditional investigative methods, including the use of informants, community/family tips, are actually far more effective. 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.[9] 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.

12. The Committee asks about the distinction between the content of communications (as made available via interception) and the record of a communication (termed 'metadata' or 'communications data'). The distinction is best explained by reference to the traditional postal distinction between the address on an envelope and its contents. However this distinction has been eroded by modern internet and mobile phone usage. Communications data includes each individual

---

[7] *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/.

[8] *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

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

URL visited, the time a phone call is made or email sent, the identity and location of senders and recipients of calls and emails, the content of messages posted on social media sites, etc. This can build an incredibly intimate picture of someone's life – their relationships, habits, preferences, political views, medical concerns and the streets they walk. To give an idea of just how much the communications landscape has changed, in 2013, statistics revealed that 73% of adults in the UK accessed the internet every day – that's 20 million more daily users than in 2006 when these figures first began to be collected.[10] We're also accessing the internet in different ways, with the number of us accessing the internet on our mobile phones more than doubling between 2010 and 2013.[11]

13. The intrusive nature of modern communications data has recently been recognised by a US federal judge in a ruling challenging the NSA's bulk metadata collection on US citizens. In *Smith v Maryland* (1979) the US Supreme Court found that there was no expectation of privacy for telephone metadata held by companies as business records. The Court found that such records didn't fall within the ambit of the Fourth Amendment and that a warrant was not required to obtain the information. However on 16 December 2013 US District of Colombia Judge Richard J Leon found that a lawsuit challenging NSA bulk metadata collection demonstrated a "substantial likelihood of success".[12] He said "*When do present-day circumstances — the evolutions in the government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies — become so thoroughly unlike those considered by the Supreme Court thirty-four years ago, that a precedent like Smith does not apply?…The answer, unfortunately for the government, is now.*" Describing the change in circumstances he described modern-day metadata as "*unlike anything that could have been conceived in 1979*" and said "*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 analyzing it without prior judicial approval…Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth*

[10] Since the Office for National Statistics started to collect figures in internet usage in 2006, 20 million more people in the UK have gone online. 36 million people, not counting the many young people who are regular users, 20 million more than when this data started to be collected in 2006.

[11] Office for National Statistics, up from 24% in 2010 to 53% in 2013: http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2013/stb-ia-2013.html.

[12] Klayman v Obama 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/.

Amendment." The ruling, which will now be subject to appeal, marks the first time a federal judge in open court has considered the collection of metadata not involving a criminal defendant.

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.

14. No. The legal framework governing the agencies' access to communication content *and* communications data is neither fit for purpose nor in compliance with requirements of the ECHR.

15. The extent to which our legal framework is wanting is difficult to ascertain without greater clarity over the agencies' interpretation of the law and what the law presently allows. While we know which laws apply (namely the Security Service Act 1989 Intelligence Services Act 1994, the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000) these laws are broadly framed and their legal interpretation by the IPT is generally not made public. The Tribunal predominantly hears cases in secret and doesn't give reasons for its judgments. Liberty has a claim pending in the IPT relating to suspected surveillance of our communications. The claim seeks to establish (a) whether the RIPA definition of 'external communication' in section 20 provides sufficient clarity concerning conditions and circumstances in which UK residents are liable to have their communications intercepted and (b) what, if any legal frameworks govern the granting of, access to, or receipt of, intercept product and communications data to/from a foreign intelligence service in respect of communications originating from or received in the UK. In advance of a legal determination on these issues we can nevertheless identify areas where we believe the law is presently lacking.

Interception

16. 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.[13] 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

[13] Section 2 RIPA.

Director-General of the Security Service, Chief of SIS and Director of GCHQ. Warrants are issued by the Secretary of State where she considers it necessary and proportionate to do so in the interests of national security; prevention and detection of crime or to safeguard economic wellbeing of the UK.

17. Section 5 RIPA requires individual interception warrants for interception of those present in the UK (hereafter 'internal interception'). An internal interception warrant must *name or describe a person or single set of premises to be intercepted*.[14] Section 8(4) RIPA also allows for the interception of 'external communications'[15] - a communication either sent or received outside the British Islands and a communication that is both sent and received outside the British Islands whether or not it passes through in the course of transit.[16] Interception of external communications is very loosely controlled – a warrant does not need to identify specific individuals or premises but need only contain descriptions of intercepted material. There is no upper limit on the number of external communications which may fall within the s8(4) regime. S8(4) warrants last for either 3 or 6 months and can be renewed indefinitely. We understand that the agencies interpret this to allow interception of any communication with a certain keyword or between a group of individuals; possibly even to cover all communications emanating from or received in a particular country. We believe (particularly in light of the Tempora reports) that external interception warrants may even authorise 'all communications leaving the British Islands'.

18. 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'[17] and disproportionate. *Liberty v UK* concerned 'external communications' interception by the Ministry of Defence of Liberty's telephone, fax and email communications between 1990 and 1997. This took place under the pre-RIPA legislation that allowed interception to cover '*such external communications as are described in the warrant'.*[18] The 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. The framework for 'external interception'

[14] Section 8(1) RIPA.
[15] Sections 8(4)-(6) RIPA.
[16] Section 20 RIPA and section 5.1 of the Interception Code of Practice issued under section 71 RIPA.
[17] Malone v UK (Application No 8691/79)
[18] Interception of Communications Act 1985.

under RIPA is strikingly similar in this respect and will almost certainly fall foul of Article 8 on the same grounds.[19] 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".*[20]

19. Of further concern is the lack of clarity around what falls within the 'external communication' definition. In particular whether it captures a call or email between two people in the UK that is routed via a server based abroad. Section 20 states that external communication is "a communication sent or received outside the British Islands" and para 5.1 of the Code of Practices states that "they *do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route*".[21] While this may appear to rule out emails and phone calls sent and received within the UK (even if routed elsewhere) it doesn't provide necessary clarity in respect of internet-based communications (eg. Google search, Youtube link, Facebook post, direct message on Twitter) where the user is in the UK but the website is based in Northern California. Terms such as 'transit' and 'en route' are inappropriate for a framework intended to regulate surveillance of web-based services. Given the default secrecy of IPT hearings and judgments on matters of law we don't know whether this point of law has ever been considered by the Tribunal, let alone decided in relation to the host of different mechanisms by which communications are transmitted in the modern age.

20. Interception powers are further extended by section 5(6) which allows conduct authorised by an interception warrant to include authorisation to *intercept*

---

[19] The Court has since considered interception under RIPA in *Kennedy v UK (Application No 26839/05).* However, this case concerned the RIPA framework for *internal* interception. The Court noted that internal interception must specify the persons or premises targeted and that '*indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA*" and was not prepared to find a violation of Article 8. This can be clearly distinguished from what is permitted for the purposes of 'external interception' under RIPA.

[20] 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.

[21] At Chapter 5, page 22, issued pursuant to Section 71 RIPA.

and obtain communications data for *communications not identified in the warrant* so far as necessary to do what is expressly authorised by the warrant. In principle RIPA then grants an unrestricted power to intercept any communication in order to give effect to authorised interceptions. Liberty understands that as it may be technically impossible to separate internal and external communications, GCHQ may be applying this power to grant itself the ability to intercept vast swathes of unwarranted internal communications to enable access to broad categories of authorised external communications.

21. This ambiguity about the scope of 'external interception' interception is confirmed by Tempora reports that vast numbers of internal communications are being intercepted –

> *There is a particular concern that the programme allows GCHQ to break the boundary which stopped it engaging in the bulk interception of internal UK communications. The RIPA requirement that one end of a communication must be outside the UK was a significant restriction when it was applied to phone calls using satellites, but it is no longer effective in the world of fibre-optic cables….the [Security Service] source said 'At one point I was told that we were getting 85% of all UK domestic traffic – voice, internet, all of it – via these international cables".*[22]

22. The external interception regime is unfit for purpose. It provides seriously insufficient clarity concerning the conditions and circumstances in which UK residents and those residing outside of the UK are liable to have their communications intercepted. Moreover the reported extent of 'external interception' under Tempora (i.e. some 600 million phone hits a day) means it could not sensibly be described as proportionate or necessary in a democratic society.

Acquisition of communications data

23. Section 22 RIPA authorises the acquisition of communications data. Under the legal framework a number of public bodies (including GCHQ) are able to internally authorise their access to communications data for a range of purposes.[23] As with 'external interceptions' RIPA does not require that authorisations specify a

[22] "MI5 feared GCHQ went 'too far' over phone and internet monitoring, *The Guardian*, 22 June 2013.
[23] Chapter 2, RIPA.

named individual. In the absence of any such criteria it is foreseeable that GCHQ authorises itself to acquire communications data for wide ranging *categories* of communications data – concerning both internal and external communications. This may include 'communications data for all individuals in X area of the country' or 'all communications data relating to X computer program or X service provider in the UK'. The only potential restrictions on this power are the requirements of necessity and proportionality. However the reported scale of GCHQ interception seems to suggest that the organisation does not sensibly interpret and apply these criteria in a lawful manner. There is no reason to think these criteria are being properly applied in relation to communications data. In any event the lack of statutory controls on the acquisition of communications data (as it applies to the security agencies *and* other public bodies) is unlawful and unfit for purpose.

Intelligence sharing regime

24. The sharing of surveillance data between the UK and foreign intelligence agencies is not provided for in law. While various pieces of primary legislation - the SSA, ISA, HRA, RIPA and DPA - are in play, none reveal with any certainty the policies and procedures that govern the circumstances in which the security agencies can obtain surveillance data from foreign intelligence partners nor disclose it. It is therefore unclear in what circumstances the UK may seek to access or disclose intercept product or communications data on particular individuals (in the UK or elsewhere) and what (if anything) the law requires in order for it to do so.

25. Under RIPA, UK agencies are not required to seek RIPA authorisation when requesting interception or communications data from foreign agencies. We are therefore concerned that current surveillance data-sharing arrangements allow UK agencies to effectively circumvent domestic legal controls on interception and acquisition of communications data.

26. When the ISC considered this issue in July 2013 it focused exclusively on the receipt of intercept product and concluded "*It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded.*"[24] The ISC further concluded that where *specified* information

[24] Intelligence & Security Committee Statement on GCHQ's alleged interception of communications under the US Prism Programme, ISC, July 2013.

was sought from the US, a Home Secretary warrant for interception was already in place.

27. These conclusions are vague and caveated. They do not confirm that circumvention has not taken place *at all* but rather that there is no evidence of this in the documents the ISC has been permitted to view. Further, the fact that individual warrants were in place for *specified* interception sought from another power does not confirm whether GCHQ considers itself bound to obtain such a warrant nor whether the UK considers itself able to make *generalised* interception requests without warrant (e.g. concerning keywords; categories of individuals) to foreign agencies that will affect UK communications. If so, this would in principle allow for unwarranted mass interception of in-country communications of UK residents. The Committee's statement also didn't address the concern that GCHQ obtains *unsolicited* surveillance data on UK residents from the US. US law allows unrestricted surveillance on UK residents[25] and the fact that most electronic communications flow through US servers means that mass UK surveillance by the US is technically possible. In his statement to Parliament in response to the initial Snowden disclosures on 10 June 2013 the Foreign Secretary said *"Since the 1940s, GCHQ and its American equivalents – now the NSA – have had a relationship that is unique in the world."*[26] This raises the real possibility that the UK may, unsolicited, receive bulk data on UK communications from its US counterpart.

28. The legal framework also appears to impose no specific controls over requests for, or unsolicited receipt of, communications data via data sharing arrangements. In theory it appears that vast quantities of communications data acquired by the US on UK residents under its permissive legal regime may be being passed – solicited or unsolicited - to the UK thus sidestepping RIPA provisions. This issue was conspicuously absent from the ISC's cursory inquiry statement.

[25] 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 FIA Court, made on an ex parte basis in closed proceedings.
[26] Ibid at footnote 4.

29. 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. The ISC has briefly considered surveillance data sharing arrangements and concluded: "*In some areas the legislation is expressed in general terms and more detailed policies and procedures have, rightly, been put in place around this work by GCHQ in order to ensure compliance with statutory obligations under the HRA. We are therefore examining the complex interaction between the ISA, the HRA and RIPA, and the policies and procedures that underpin them, further."*[27] That the formal oversight Committee describes this legal framework as 'general' and the legal position 'complex' gives an indication of present difficulties.

30. The framework for disclosure of surveillance data to foreign agencies is similarly loose and permissive and takes place outside any recognisable legal framework. It appears that under RIPA, GCHQ is in principle entitled to transfer intercept product and communications data concerning UK residents to the NSA and other intelligence partners where the Secretary of State is satisfied that mechanisms for storage and destruction of data are suitable.[28] Transfer of data in this way is a fresh interference with Article 8 and the lack of statutory framework setting out a policy, process and safeguards for such disclosures means that the practice is not in accordance with law.

31. Article 8 further requires that data transfers are necessary in a democratic society and proportionate. The reported scale of interception of 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.*

[27] Ibid at footnote 24.
[28] Section 15(6) and (7) RIPA and relevant Code of Practice guidance.

There is a further concern. The Government has chosen to 'neither confirm nor deny' the allegation that it shares information with the Americans to facilitate drone strikes outside of a conventional conflict scenario.[29] In her Legal Advice 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 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."*[30]

(c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

32. The lack of clarity about what is presently permitted by law and the authorities' interpretation of law makes this a difficult question to address. However there are a number of areas where reforms are clearly required and below we make some initial recommendations as to where they should be focussed -

a) The current definition of 'external communication' cannot be maintained. The power presently appears to allow blanket interception of all communications entering or leaving the UK and all communications between two people outside of the UK. This is not targeted surveillance and is not necessary or proportionate in a democratic society. It is unclear that there is any justification for a legal distinction between 'internal' and 'external' communications. There appears to be no reason of principle for different procedural safeguards attaching to requests for the interception of internal communications and communications either sent or received outside the UK. In a globalised world where people routinely and regularly call, text, email and Skype across national borders any outdated notions that 'external communications' were by their nature more likely to be suspicious or less

[29] *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."*
[30] Ibid at footnote 24, para 84.

worthy of protection are redundant. There seems to be no reason why a UK resident should have less privacy protection for emails and phone-calls sent or made to people abroad than for their domestic equivalents. Similarly interceptions that would catch the calls and emails of a UK citizen while on holiday abroad should not be subject to a lower threshold of scrutiny than those which would catch his/her emails and calls while in the UK. Further maintaining this distinction discriminates against those who communicate more regularly with those outside the UK, perhaps by reason of nationality, ethnicity, age etc. Requests for interception must be specific, targeted and proportionately circumscribed wherever a person is in the world. The present legal distinction is further undermined by the fact that it is no longer technically feasible to distinguish between external and internal communications.

b) The legal distinction between the 'content' of communications and 'communications data' cannot be maintained. The distinction is not fit for the mobile phone and internet age and the different legal regimes that apply to the acquisition of this surveillance data must be harmonised. In particular, requests for communications data must be specific in nature and externally authorised.

c) All targeted surveillance (including interception, acquisition of communications data, use of covert human intelligence sources, bugging) must be pre-authorised by a serving judge. 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 will improve public trust and confidence in the system of surveillance. 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 targeted surveillance practices permitted under RIPA. Prior to the Snowden disclosures there has been huge public concern about the Metropolitan Police's use of undercover officers to infiltrate peaceful environmental groups and the family of Baroness Doreen Lawrence. This badly regulated practice has led to collapsed prosecutions and convictions overturned. It has also led

to gross privacy violations and untold harm. These scandals demonstrate the fatal problems of internal authorisation as currently permitted by a number of RIPA surveillance techniques. Political authorisation (as required for interception) suffers the same flaws. 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".*[31] 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."*[32]

d) 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' sensitive data including that of UK residents. The legal framework for the transfer of suspects between countries is publicly known, by way of extradition treaties and legislation. So too should arrangements that relate to the agencies' powers to disclose and receive surveillance information.

e) The ex post facto oversight of the security services provided by the Surveillance Commissioners, the IPT and the ISC is gravely lacking. Pre-judicial authorisation of targeted surveillance should help plug this oversight gap. However there are many reforms that could be made to this tripartite oversight regime to improve transparency and accountability while preserving

[31] *Klass and others v Federal Republic of Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978
[32] David Bickford CB, European Parliament Libe Enquiry, Judicial Scrutiny of Intelligence Agencies, 7 November 2013.

national security. There is not space in this brief response to detail the range of reform options but, by way of example, the powers of IPT could be reformed to require public hearings and published judgments unless national security demands secrecy; and to give the Tribunal the power to issue a declaration of incompatibility under the HRA.

Isabella Sankey