LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on *'A Question of Trust: The Report of the Investigatory Powers Review'*

June 2015

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

Bella 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 report of the Government's Reviewer of Terrorism's investigatory powers review. The report condemns the status quo under the Regulation of Investigatory Powers Act 2008 as *"undemocratic, unnecessary and – in the long run – intolerable"*[1] and advises that it - along with a number of other statutes granting investigatory capabilities - be replaced with a comprehensive new law[2] that can be properly understood by parliamentarians and the public alike.[3] He recommends that the new law should prohibit the use of any other powers providing for the interference of communications[4] and sets out that existing and future intrusive capabilities should be avowed to the Secretary of State and then publicly avowed at the earliest possible opportunity.[5] This stark and realistic assessment of the need for transparency and reform is in glaring contrast to the Government's repeated claims since 2013 that the current legislative framework contains effective safeguards to properly protect our privacy.

2. For almost a decade, Liberty has argued that the substance, format, and oversight arrangements for the UK's surveillance regime are in need of urgent and radical overhaul. We are delighted that a number of the changes we have advocated, including in our written evidence to this review, have been recommended in the report. In particular, we welcome the view that no case has been made for new powers – including those previously contained in the Draft Communications Data Bill (DCDB) – but there is a need for new safeguards; the recognition that in an international world the UK Government must not propose for itself powers that we would not wish to see adopted by other countries and the vital importance of ensuring respect for our international human rights obligations[6]; and the requirement –as is the case in democratic countries across the globe – that warrants to intercept communications be granted by judges rather than politicians.[7]

3. Liberty supports the targeted and proportionate use of lawful intrusive powers. But the Snowden revelations of 2013 and subsequent litigation brought by Liberty and others shows how far we have moved from a model whereby those under suspicion are targeted and the innocent are left free from state intrusion. Even more worrying is the fact that prior to

[1] Paragraph 35.
[2] Recommendations 1, 2, 5, 6 and 7.
[3] Recommendations 3 and 4.
[4] Recommendation 7.
[5] Recommendation 9.
[6] Paragraph 1.9(d).
[7] Recommendation 22.

the revelations, the public and politicians were unaware of the nature and extent of blanket surveillance. In order for trust to be restored, Parliament must assert its democratic function and set clear limits to the use of intrusive powers and prohibit their use on a mass scale. Safeguards are vital, but Parliament must challenge the undemocratic nature of mass surveillance too.

4. The inadequacy of our surveillance laws and the need for both online and offline reform has been laid bare in some of rare instances in which surveillance has come to light. In recent years, the Metropolitan police circumvented PACE safeguards to access the phone records of journalists, spied on a grieving Baroness Lawrence and her family and infiltrated social and environmental justice groups to the extent that women were tricked into serious and long-term romantic relationships – one even giving birth to a child with undercover officer. These uncontrolled activities have wrecked lives, led to miscarriages of justice and abandoned prosecutions. The Government cannot continue to claim that the current surveillance regime does no harm to the innocent – that is clearly not the case. Over the same period, public interest litigation has revealed how GCHQ intercepted the legally privileged communications of a torture victim challenging MI6 complicity in his kidnap to Gadaffi's Libya[8] and further intercepted the communications of human rights NGOs in South Africa and Egypt.[9] What kind of signal are British authorities sending to despotic regimes and those who risk their lives to challenge them all over the world? The use of covert human intelligence sources (CHIS), the increased use of hacking and attempts to defeat encryption - none which were within the scope of the Anderson review – must all now be considered by Parliament and made subject to a requirement that they are targeted and subject to increased safeguards.

No case for the Snoopers' Charter

5. The Home Office has been pursuing what has been described by an insider as a *"woefully unevidenced"* plan for extended mass retention of the population's communications data since 2008.[10] In 2009 the department published a consultation proposing among other options a centralised government database of all our communications data.[11] This plan was

[8] Belhadj and Others v Security Services and Others, Respondents' revised response to the claimants' request for further information, published 6 November 2014.
[9] Liberty and Others v GCHQ and others, 22 June 2015.
[10] There is no real case for a snoopers' charter – but that won't stop it, Tim Colbourne, The Guardian, 14 June 2015.
[11] Liberty's response to the Home Office consultation 2009 is available here - https://www.liberty-human-rights.org.uk/sites/default/files/liberty-s-communications-data-consultation-response.pdf

abandoned and in 2010 the Coalition Government initially appeared to take a different tack, pledging to "*end the unnecessary retention of records of emails and phone calls*" seemingly referring to the blanket data retention provisions of the EU Directive that came into force the previous year. However, before long the Home Office appeared to win out and the DCDB (dubbed the "Snoopers' Charter") was published, proposing mandatory retention of subscriber data, blanket retention of weblogs, third party data and the creation of a "request filter" which would allow the processing and profiling of the customers communications data by communication service providers (CSPs). The parliamentary committee convened for its scrutiny ultimately rejected the draft Bill following expert evidence including from law enforcement and receiving written objections from over 19 000 people.

6. The Home Office's approach to its quest for greater blanket retention powers has been characterised by a lack of genuine engagement and openness. The Reviewer notes that consultation with law enforcement and CSPs seems to have been non-existent over the past few years and the same is true for civil society - Liberty's last contact with the Home Office pre-dates the publication of the 2012 draft Bill. The Reviewer confirms that a further Bill was drafted in 2013, which he has been shown, but says that this Bill has not be made publicly available; nor shared with civil society organisations, law enforcement or the CSPs. The Reviewer also notes that consideration of the DCDB predated the Snowden disclosures of 2013 and as chair of the Committee Lord Blencathra complained following the disclosures, the overlapping capabilities of the Prism and Tempora programmes revealed were "*highly, highly relevant*" to consideration of the draft Bill but had not been disclosed to the Committee.

7. The Reviewer identifies that since the joint committee rejected the 2012 draft Bill there have been significant developments. The Court of Justice of the European Union (CJEU) has ruled in *Digital Rights Ireland*, making clear that the previous (and in our view current) regime for data retention in the UK is unlawful, let alone the more intrusive capabilities planned.[12] The Reviewer also observes that the utility of the request filter and collection of third party data is now thrown into doubt by technological developments (including increased encryption following Snowden). Despite the heightened political rhetoric of the Home Secretary towards the end of the Coalition's administration, the Reviewer reports that "*as to the compulsory retention of third party data – an extremely expensive part of the planned Communications Data Bill – I did not get the sense that this was judged to be the priority that is once was, even within law enforcement. The CSPs I spoke to about it were*

[12] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).

either actively hostile or felt remote from the debate since it was so long since they had been consulted".[13]

Web logs, third party retention of data and request filter

8. The Reviewer is clearly highly sceptical about whether an operational case exists for web logs in the fluid and fast changing world of communications technology and even then whether it could possibility meet the legal requirements of proportionality. He recommends that:

> *"Government should initiate an early and intensive dialogue with law enforcement and CSPs in order to formulate an updated and coordinated position, informed by legal and technical advice, on the operational case for adding web logs to the data categories currently specified in the Schedule to the Data Retention Regulations 2014."*[14]

He adds that*:*

> *"full consideration should be given to alternative means of achieving those purposes, including existing powers, and to the categories of data should be required to be retained, which should be minimally intrusive. If a sufficiently compelling operational case has been made out, a rigorous assessment should then be conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained. No detailed proposals should be put forward until that exercise has been performed."*

9. Web logs were never defined in the draft Bill but according to David Anderson the Home Office defines them as "*a record of the interaction that a user of the internet has with other computers connected to the internet*". As a former special adviser to the former Deputy PM has observed:

> "*this covers a ludicrously vast range of activities, including opening an app on your phone, logging on to a virtual private network, editing a spreadsheet in Google docs or uploading a photo to iCloud. It is a carte blanche to store any kind of data that the Government chooses to ask for"*.[15]

[13] Paragraph 14.37.
[14] Paragraph 15.
[15] See footnote 10.

The Reviewer acknowledges the invasiveness of the proposal (for example how web log retention could reveal that a user "*has visited a site for sufferers of a particular medical condition*") and says that it is widely accepted in the law enforcement community that "*the compulsory retention of web logs would be potentially intrusive; the political environment not to mention the legal environment may not be conducive and that there would be expense and complexity involved in making these changes that would only be justified if any new power were to be extensively used".*[16] He reveals that unlike submissions made by law enforcement to the DCDB Committee, it was not submitted to him that access to web logs is essential.

He goes even further on the issue of third party data, saying

> *"there should be no question of progressing proposals for the compulsory retention of third party data before such a time as a compelling operational case may have been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions is currently satisfied."*[17]

He further reports that UK CSPs remain sceptical about this proposal and that in a post-Snowden world the utility of the proposal needs to be re-assessed, particularly in view of the high anticipated cost.

10. The Reviewer's report also provides a useful and telling comparative overview on the issue of mandatory web log and third party data retention:

> "*I am aware of no other Five Eyes or European country that provides for the compulsory retention either of web logs or of third party data. Such obligations were not considered politically conceivable by my interlocutors in Germany, Canada or the US. The 2015 Australian data retention law specifically exempts both web logs and third party data from the categories of data that must be retained by CSPs…Against that legal, technical and comparative background, it seems to me that a high degree of caution is in order".*[18]

Elsewhere in the report he adds that he is not aware of any other Commonwealth country in which service providers are required to retain web logs.

[16] Paragraph 9.60.
[17] Paragraph 18.
[18] Paragraph 14.30.

11. These conclusions support Liberty's alternative recommendation for an improvement to the MLAT regime to ensure a feasible and lawful model of data exchange in a world where communications are said to be "going dark" i.e. increasingly encrypted and held by communications service providers outside of the jurisdiction. Instead of creating expensive and ever more intrusive capabilities (e.g. web log and third party retention) the Government would be better advised to work to improve their existing capability to achieve access to this data from outside the jurisdiction.

Current system for communications data retention and access

12. In April 2014 the CJEU ruled in *Digital Rights Ireland* that the EU Data Retention Directive which mandated blanket data retention between 6 -24 months was invalid due to its sweeping in its interference with privacy rights.[19] The judgment made clear that existing UK legislation, including the access regime under the RIPA required urgent review. The CJEU acknowledge the important role of data retention and access to the prevention and detection of serious crime and laid out the following ten principles to ensure compliance with human rights standards –

a. restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);
b. provide exceptions for persons whose communications are subject to an obligation of professional secrecy (paragraph 58);
c. distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
d. ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);
e. empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);
f. restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);
g. limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);
h. ensure the data is kept securely with sufficient safeguards to secure effective

[19] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).

protection against the risk of abuse and unlawful access (paragraph 66);

i. ensure destruction of the data when it is no longer required (paragraph 67); and
j. ensure the data is kept within the EU (paragraph 68).

13. Three months after the judgment, the UK Government responded with emergency legislation – the *Data Retention and Investigatory Powers Act 2014* (DRIPA) - which was rushed onto the statute book in 7 days in July 2014. DRIPA allows the Secretary of State to order communications companies to retain all communications data for 12 months – no link with the prevention or detection of serious crime is required.[20] It potentially catches the communications of everyone in the UK including the emails, calls, texts and location information of MPs, journalists, lawyers, doctors and other communications that may be confidential or privileged.[21] The Act also failed to narrow the loose and lax communications data access regime for public authorities' provided by Chapter 2 of RIPA and under the section 25(1) *Regulation of Investigatory Powers (Communications Data) Order 2010*. The law currently authorises the acquisition of communications data by hundreds of public authorities and most public bodies are able to authorise internally their access to communications data for the same broad range of purposes under which communications data is retained which go much further than the detection and prevention of serious crime. Barring local authority access, there is no requirement for independent prior judicial authorisation when communications data is sought by public bodies.[22]

14. Liberty supports the important role of communications data in missing persons situations, preventing and investigating serious crime, securing convictions as well as acquitting the innocent. We do not believe however that the useful role of communications data in the investigation of crime, justifies the blanket retention of the data of the entire population and the lax access regime that currently exists under RIPA. The volume of communications data used in such investigations is a tiny fraction of that retained – at huge cost – on millions of innocent people. Moreover it would be entirely feasible to construct a

[20] Part 3 of the CTSA 2015 extended the scope of compulsory data retention to include the data that are needed to link an IP address with a device that was using that address at a particular time. However, subsection (3)(c) DRIPA specifically excluded the ability to retain weblogs.
[21] While the Wilson doctrine may provide some protection against the interception of content of an MPs communications, the Government has stated that the doctrine does not apply to communications data (HC Deb, 12 March 2014, column 306). The Government also claims that communications data should not be considered legally privileged.
[22] Section 37 of the *Protection of Freedoms Act 2012* introduced a requirement for prior judicial authorisation for access to communications data by local authorities. The Government has offered no explanation as to why this safeguard should not be mandatory for all communications data access requests.

framework, which allowed for the targeted retention of, and access to, communications data of suspects or in relation to particular law enforcement operations.

15. Liberty is currently representing David Davis MP and Tom Watson MP in their legal challenge to DRIPA. They have asked the High Court to either make a declaration of incompatibility under section 4 of the Human Rights Act or to disapply section 1 DRIPA for its incompatibility with the EU Charter. The Reviewer notes in his report that "*the extent to which current law gives effect to the requirements of Digital Rights Ireland is disputed in the MPs' case…which will be heard in the High Court in June 2015. In the circumstances it would be inappropriate for me to venture an opinion on its legal compatibility".* DRIPA is set to expire at the end of 2016 but given that the High Court is currently considering the MPs challenge, Liberty urges parliamentarians to urgently begin the process of considering its replacement.

16. Prior to the decision in *Digital Rights Ireland*, several courts across Europe had annulled their countries legislation implementing the EU Directive– Bulgaria, Romania, Germany, Cyprus, Czech Republic. Since the DRI judgment three more countries have struck down blanket data retention legislation including Austria, Slovenia, Romania and most recently, Belgium.

Judicial authorisation

17. The UK is currently alone amongst the Five Eyes nations in making no use of judges for the prior authorisation of interception warrants. We welcome, as a huge step forward in the debate on state surveillance, the Reviewer's recommendation that interception warrants be judicial rather than political. It is further significant that he describes this as the easiest conclusion of all for him to reach.[23] Under the model proposed in the Report, the new Independent Surveillance and Intelligence Commission would include senior serving or retired judges appointed to act as Judicial Commissioners. Judicial Commissioners would be responsible for the authorisation of all interceptions and of the bulk collection of communications data. An appeal against a refusal to authorise would lie to the Chief Judicial Commissioner. Where an application for interception is made for the purpose of national security and the Home Secretary certifies that the warrant is required in the interests of the defence and/ or foreign policy of the UK, the Judicial Commissioner would only be able to

[23] Paragraph 14.48.

depart from the certificate on the basis of the principles applicable in judicial review. The model proposed in the report would include arrangements for the prompt consideration of urgent applications.[24]

18. The Reviewer sites a number of reasons for recommending a system of judicial warrants, including: *"the remarkable fact (at least to an outsider) that the Home Secretary routinely signs thousands of warrants per year"* in addition to the many other varied and broad-ranging functions of her Office.[25] Significantly he further considers that public confidence in the system could be greatly improved by the introduction of prior judicial authorisation. Whilst the Reviewer does not doubt that the current Home Secretary uses her powers in good faith, he points out that *"neither the British public nor the global public can be expected to take the probity of the Secretary of State on trust"*.[26] Similar concerns exist amongst communications service providers and in evidence to the Review many, and particularly those operating under the US system of judicial warrants, were concerned about responding to Secretary of State warrants. The report quotes one provider as specifying that *"the UK is in a minority with political authorisation, and perceptions do matter"*.[27] The Reviewer further points to the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union in support of a system of prior judicial authorisation and refers to the existence of established systems for judicial approval in the context of property interference and long-term, undercover policing operations.[28]

19. It is the proper constitutional function of the independent judiciary to act as a check on the use of State power. Judges are best suited to applying legal tests to ensure that surveillance is necessary and proportionate and their involvement would vastly 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. There is evidence from other comparable jurisdictions that requiring independent judicial authorisation for interception warrants is a workable system. In America,[29] federal investigative or law

[24] For example, recommendation 32.
[25] Paragraph 14.48.
[26] Paragraph 14.50.
[27] Paragraph 11.19.
[28] Paragraph 14.50.
[29] 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*

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.[30] In Canada it is unlawful to intercept private communications unless the interception is in accordance with an authorisation issued by a judge,[31] 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.[32]

20. 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. 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.[33] 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[34], the Joint Committee on Human Rights[35], three former Directors of Public Prosecutions[36], a former Attorney General and even the former director of M15 Dame Stella Rimington[37] have reached the conclusion that intercept can and should be used. However successive Privy Council reviews have rejected the proposal, most recently on cost grounds.[38] The Reviewer considered the bar on the admissibility of intercept evidence to be outside the scope of the Report, however, he points to the fact that this restriction means a premium is placed on obtaining content by other

---

PATRIOT Reauthorization Acts in 2006, and by the *Foreign Intelligence Surveillance Act (FISA) Amendments Act* of 2008.

[30] *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).

[31] Canada *Criminal Code*, Part VI, section 186.

[32] Part 11A of the *Crimes Act*, and under the *Misuse of Drugs Amendment Act 1978*.

[33] The Guardian, *'Leaked memos reveal GCHQ efforts to keep mass surveillance secret'*, 25 October 2013.

[34] 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.

[35] 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.

[36] 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'.

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

[38] Rt Hon James Brokenshire MP, Commons Hansard, 17 Dec 2014 : Column 99WS.

means and encourages excessive reliance on communications data to prosecute crime. He points out that the content of a computer or phone is frequently admitted in evidence as is foreign intercept product.[39]

21. In terms of practicalities of judicial oversight, the report recommends that an Independent Surveillance and Intelligence Commission (ISIC) should replace the offices of the three current oversight Commissioners. ISIC should take over the existing auditing functions of its predecessor Commissioners, and additional functions relating in particular to the acquisition and use of communications data, the use of open-source intelligence and the sharing and transfer of intercepted material and data. Through its Judicial Commissioners, who should be serving or retired senior judges, ISIC should also take over the judicial authorisation of all warrants.[40] We welcome these efforts to strengthen oversight of the work of the law enforcement and security agencies.

Computer network exploitation (aka hacking)

22. As the Reviewer observes, CNE was only first "avowed" in the UK by the publication of the draft Equipment Interference Code of Practice (pursuant to section 71 RIPA) in February 2015.[41] This consultation was published in response to cases lodged by Privacy International and a collective of internet and communications services in the IPT challenging the practices disclosed in the Snowden files.[42] There is currently no clear or accessible legal regime governing the hacking of property and devices by the Intelligence Services. Government relies on enabling powers contained in sections 5 and 7 of the *Intelligence Services Act 1994* (ISA). Section 5 covers activity in the UK and provides that a warrant authorised and issued by the Secretary of State may make lawful any "*entry on or interference with property or with wireless telegraphy*". Section 7 ISA (sometimes referred to as the 'James Bond' clause) covers operations outside the UK. It allows the Secretary of State to sign an authorisation that removes civil and criminal liability for activity which may otherwise be lawful under UK law. The ISC report confirms that GCHQ and SIS obtain

[39] Paragraph 9.18.
[40] Recommendations 28 -30.
[41] Liberty's response to the Home Office Equipment Interference consultation is available here - https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%27s%20response%20to%20the%20Home%20Office%20consultation%20on%20the%20Equipment%20Interference%20Code%20of%20Practice%20%28Mar%202015%29.pdf.
[42] Greennet Limited, RiseUp Networks Inc, Mango Email Service, Korean Progressive Network, Greenhost, Media Jumpstart Inc and Chaos Computer Club.

"class-based" authorisations under section 7 ISA enabling them to undertake *classes of activities* overseas that might otherwise be unlawful.

23. Hacking enables the State to conduct the most comprehensive form of surveillance imaginable and has the potential to compromise and destroy the security of individual devices and networks affected as well as the entire internet. The Open Rights Group have described the power in the following terms –

> *"The intelligence agent can access any stored data, including documents, emails, diaries, contacts, photographs, internet messaging chat logs, and location records on mobile equipment. He can see anything typed into the device, including login details and passwords, internet browsing histories and draft documents and communications the user never intended to share. He can recover files that have been deleted. He can control any functionality, including surreptitiously turning on the microphone, webcam and GPS-based locator technology. He can even re-write the code that controls the device, adding new capabilities and erasing any trace of his intrusion. And he can overcome any attempts by the user to protect her privacy, not only by accessing information that was never meant to be shared, but also by overcoming encryption and secure communications methods."*[43]

24. Invasive hacking techniques are being used not only against intelligence targets but also against innocent individuals and key global infrastructure networks to enable mass surveillance. According to analysis of the Snowden files by The Intercept news site, the computer systems of a Belgian telecommunications provider were infected by GCHQ with malware which allowed GCHQ to access private communications passing over the Belgacom network. To do this, GCHQ targeted individual engineers working for Belgacom and infected their electronic devices, resulting in the engineers going to a fake website masquerading as the Linked-in website which attacked the engineers' computers. This technique, known as QUANTUM, allowed GCHQ to have control of the computers and access the Belgacom networks. This industrial hack went undetected for two years.

25. Hacking has the unique potential to cause widespread damage and, by compromising the security of devices and networks, further criminal enterprises. For this reason full parliamentary debate on its use is required and at the very least legal safeguards introduced that at least mirror the legal safeguards recommended for interception.

[43] Ibid.

International intelligence sharing

26. The report describes an *"international trade in intelligence"* between the "five eye" partners of UK, USA, Canada, Australia and New Zealand and beyond.[44] However the legal authorities for sharing information, the process to be followed and the safeguards in place are not set out clearly – or in some instances not set out at all - in legislation.

27. Insofar as material gathered by the British services is shared with other countries, the report explains that the security services take the view that under their founding statutes, information can be shared if it is *"necessary for the purpose of the proper discharge of the security and intelligence agencies' functions"* and that when it is considered that this test is met certain RIPA safeguards apply. However, the report concludes that *"in practical terms, the safeguards applying to the use of such data are entirely subject to the discretion of the Secretary of State."*[45] The report also states that RIPA imposes no limits on the sharing of communications data obtained from service providers with overseas governments, although the Acquisition Code provides some guidance for dealing with requests for information.[46]

28. The report also sets out that RIPA and the Codes of Practices are silent on British services receiving or accessing information from foreign services, with the security services only limited by the "general constraints" on their actions in various statutes.[47] It was only during the course of Liberty's legal action against the security services in the IPT that information about the way in which the security services approach such situations was revealed. In a landmark decision, the ITP held that prior to these disclosures, the framework for information sharing was not sufficiently foreseeable and was not therefore "in accordance with law". The Tribunal held that as a result of the fact that the litigation had resulted in disclosures of information, the security services were no longer acting unlawfully when accessing information from the US. It is wholly unacceptable that it requires litigation by an NGO that was only made possible by revelations made by a whistle-blower to render the actions of the security services lawful.

29. The report recommends that information sharing with foreign countries be subject to strict and clearly defined and published safeguards and subject to scrutiny of the new ISIC.[48] The report adds that the *"the new law should make it clear that neither receipt nor transfer as*

[44] Paragraph 10.30.
[45] Paragraph 6.87.
[46] Paragraph 6.88.
[47] Paragraph 6.89.
[48] Recommendations 76 and 77.

referred to in recommendations 76-77 above should ever be permitted or practised for the purpose of circumventing safeguards on the use of such material in the UK".[49]

Extra-territorial legal provisions

30. The report recognises that technological developments have changed the ways in which we communicate.[50] Associated with that, the report identifies that many of those who develop and provide communications services – be it social media, emails, internet calls or other – will not necessarily have their legal base in the UK.[51] Similarly, any information that is stored by these companies may be located in different countries.[52] Liberty argues that that it is incumbent on the government to develop a system for dealing with service providers based outside the UK in a legal, principled, sustainable, and human rights compliant manner.

31. The Data Retention and Investigatory Powers Act was introduced via emergency legislation in July 2014. Section 4 DRIPA sought to deal with companies operating outside the UK by extending 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.

32. At the time DRIPA was passed, the Government sought to claim that RIPA had always had extraterritorial effect and these provisions were simply intended as clarification. This claim was both misleading and absurd. In general terms, legislation passed by the UK

[49] Recommendation 78.
[50] Paragraph 4.4 onwards.
[51] Paragraph 4.12.
[52] Paragraph 6.95.

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 made no sense. The report confirms that:

> "*Overseas service providers are generally unhappy with the assertion of extraterritoriality in DRIPA 2014, which they did not necessarily accept (despite the view of the UK Government) to have been implicit in the previous law and had not encountered in the laws of other countries. While legal compulsion was in principle preferable to voluntary compliance, it was thought that the unilateral assertion of extraterritorial effect would be met by blocking statutes, was not "scalable to a global approach" and was viewed as "a disturbing precedent" for other, more authoritarian countries."*[53]

33. The Reviewer's report notes that when countries seek to enforce legislation extraterritorially these powers may come into conflict with legal requirements in the country in which companies being asked to comply with a legal request is based or stores information. Companies explained to the reviewer that they did not consider it was their role to arbitrate between conflicting legal systems. Liberty completely agrees: the protection of vital human rights should not be left to the goodwill and judgement of a company. The report also notes principled concerns from companies:

> *"They expressed concerns that unqualified cooperation with the British government would lead to expectations of similar cooperation with authoritarian governments, which would not be in their customers', their own corporate or democratic governments' interests."*[54]

Mutual Legal Assistance Treaties

34. The alternative, most appropriate – and probably most successful way – for Government to seek to access information held overseas or by companies based 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

[53] Paragraph 11.17.
[54] Paragraph 11.24.

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.

35. The report acknowledges that the MLAT system is currently slow and cumbersome, but concludes that the Governments should *"seek the improvement and abbreviation of MLAT procedures, in particular with the US Department of Justice and the Irish authorities"* and *"take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations."*[55] The report advocates the maintenance of extraterritorial capabilities until these recommendations have been achieved. However in view of the principled objections to extraterritorial provisions along with the report's recognition that a number of overseas service providers do not consider themselves bound by them, the maintenance of these provisions is surely - at best - counter-productive.

Sir Nigel Sheinwald

36. The report notes that US technology companies and civil society both advocated the improvement of MLATs as an alternative to extraterritorial provisions. The report also refers to the work of Sir Nigel Sheinwald as Special Envoy to the Prime Minister on law-enforcement and intelligence data sharing and suggests that Sir Nigel's will be *"the decisive voice"* on this matter. On 11 June, the Prime Minister's written statement responding to the Anderson review noted: *"the Government will be taking forward Sir Nigel's advice, including pursuing a strengthened UK-US Mutual Legal Assistance Treaty process and a new international framework. As David Anderson recognises in his report, updated powers, and robust oversight, will need to form the legal basis of any new international arrangements."*[56] In order to facilitate an open and public debate about surveillance, we strongly urge parliamentarians to press the Prime Minister for publication of the Sheinwald report.

Mass v targeted surveillance

37. While Liberty supports the use and value of targeted intrusive surveillance powers, we believe that the mass speculative interception of communications and the blanket retention of communications data is unlawful, unnecessary and disproportionate. Liberty, Amnesty International, Privacy International and a number of other domestic NGOs are

[55] Recommendation 24.
[56] House of Commons: Written Statement (HCWS27)

currently challenging the lawfulness of mass interception in the European Court of Human Rights. The Reviewer acknowledges that the compatibility of the UK's regime of bulk external interception with Article 8 privacy protections is an issue awaiting determination by the Courts, adding that:

> *"It is not [his] function "to offer a legal assessment, particularly in a case that is under consideration by a senior court"*[57]

In the meantime, the report suggests that "bulk collection" of external communications should continue subject to "additional safeguards", including: (a) the introduction of prior judicial authorisation; (b) the requirement that bulk interception should only be permitted if a new "bulk communications data warrant" will not suffice; (c) greater clarity around the distinction between external and internal communication; and (d) with information-sharing between states based on clearly defined and, where possible, published safeguards.[58]

38. Whilst the central question of the legality of the UK's bulk external interception regime is yet to be resolved, in *Liberty v UK* (2008), the European Court of Human Rights found a breach of Article 8 in comparable circumstances. The case 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'*. The power was found to be too broad as it allowed the interception of almost all external communications transmitted by submarine. Yet the replacement framework for 'external interception' under section 8(4) RIPA is strikingly similar in this respect. 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"*.[59]

[57] Paragraph 14.45.
[58] Recommendations 40-49 and 72-80.
[59] 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/wpcontent/uploads/2014/01/APPG-Final.pdf.

39. Bulk interception was only first formally acknowledged in the ISC's March 2015 report. It has never been debated by Parliament, let alone voted on, but has instead been inferred by GCHQ from the vaguely worded power in section 8(4) of RIPA. It only came to public attention as a result of the Snowden disclosures. A bulk warrant is targeted at a telecommunications system rather than specific, individual persons or premises as required under section 8(1) RIPA. It allows millions of communications to be intercepted and examined each day without any requirement of suspicion nor even any discernable link to a particular operation or threat. According to the Snowden documents in 2013, GCHQ was handling 600 million telephone events per day and downloading the equivalent of 192 volumes of the British Library under section 8(4) warrants. At the end of 2014, 20 section 8(4) warrants authorizing mass interception were in place. Far from relating to the investigation of criminal activity, these vast surveillance operations seek to create what was described in a recent and highly critical report by the Civil Liberties, Justice and Home Affairs Committee of the European Parliament as a *"fully-fledged preventive state"* unrestrained by national borders.[60]

40. The intimate nature and frequency of ordinary people's modern-day internet based 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."*[61]

41. Bulk interception has also led GCHQ to intercept and examine the communications of civil liberties groups. In proceedings brought by Liberty, Privacy International, Amnesty International, ACLU and a number of other national human rights organisations from around

[60] European Parliament Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, published 21 February 2014, paragraph 5, available at - http://www.polcms.europarl.europa.eu/cmsdata/upload/73108fbabb11-4a0b-83b8-54cc99c683b5/att_20140306ATT80632-1522917198300865812.pdf.

[61] 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-internetyahoo.

the world, the Investigatory Powers Tribunal disclosed on 22nd June 2015 that the intelligence agency had intercepted and examined private communications of the Egyptian Initiative for Personal Rights (EIPR) and the Legal Resources Centre (LRC) in South Africa. It ruled that the Agency was in breach of its own secret procedures for handling information and violated the human rights of the organisations concerned. It did not make determinations concerning whether the other eight organisations had been intercepted. This follows the admission by the security services last year 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.[62]

42. Bulk interception of 'external' communications is arbitrary. The distinction between external and internal communications is a hangover from the Cold War when the authorities' focus was on the communications between foreign Governments and their agents in the UK. But in the modern world where threats to national security and serious organised crime are said to be home grown as well as located overseas, there is no principled justification for separate legal regimes that allow mass interception of cross border communications but require named persons and premises for domestic warrants. The internal/external divide allows for patently arbitrary results in the current technological environment. Last year, during the course of Liberty's litigation in the IPT, it emerged that the indiscriminate interception of UK residents' Facebook and Google communications was considered lawful by Government because they are defined as 'external communications'. The statement, from Charles Farr, the Director General of the Office for Security and Counter Terrorism, was the first time the Government had openly commented on how it thinks it can use the UK's vague surveillance legal framework to indiscriminately intercept communications through its mass interception programme, TEMPORA. The secret policy outlined by Farr defines almost all communications via Facebook and other social networking sites, as well as webmail services Hotmail and Yahoo and web searches via Google, to be 'external communications' because they use web-based 'platforms' based in the US.[63]

43. The Reviewer's treatment of the internal/ external distinction was influenced by reluctance to advocate a reduction in protection for domestic communications, however he openly accepts that external interception will necessarily pick up domestic communications

[62] *Belhadj and Others v Security Services and Others*, Respondents' revised response to the claimants '
request for further information, published 6 November 2014.
[63] Witness Statement of Charles Farr, 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.

in the process.[64] Concerns about the impact of external bulk collection on those in this county led the Reviewer to recommend that bulk interception warrants relate to the recovery of intercepted material comprising communications of those believed to have been outside at the time of the communication, clarifying the internal/ external distinction.[65]

44. The Reviewer also notes that:

> *"Though Digital Rights Ireland did not concern the bulk interception of content, it is arguable that its principles (including in relation to prior independent authorisation) should apply in that area with at least the same force."*[66]

Liberty believes that the principles articulated in Digital Rights Ireland for the retention of communications data, also apply to the more intrusive technique of interception. *Digital Rights Ireland* is part of a broader trend away from mass communications data retention and collection regimes which should inform the debate on mass interception. The USA Freedom Act, passed earlier this month, represents further significant progress. The Act reduces the capacity of the NSA to undertake mass collection of Americans' phone records, requiring instead that a subset of data be requested pursuant to limits set out in the Act.[67]

45. Aside from the disproportionality and principled dangers of blanket surveillance, its necessity has not been shown. In the USA, 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".[68] The Reviewer offers six anecdotes provided by the Agencies in an attempt at justifying mass interception. However, with the vague and limited information provided, it is impossible to assess whether the security outcomes could have been achieved by using the wealth of targeted and operation-led intrusive surveillance powers at the Agencies' disposal. In nearly all of the examples, reference is made to known terrorists or a specific "intelligence operation".

---

[64] Paragraph 14.76
[65] Ibid, paragraph 14.77.
[66] Ibid, paragraph 5.79.
[67] USA Freedom Act 2015, available at: http://judiciary.house.gov/_cache/files/1cb59778-0a72-4c09-920d-0e22bf692bb4/fisa-01-xml.pdf.
[68] 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/.

46. Affording lesser protection to cross-border communications also undermines the universality of human rights and will encourage other states to breach the privacy of British nationals in a similarly casual manner. 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. The UK should lead the way by respecting the basic rights and freedoms of nationals and non-nationals alike. Liberty will continue to call for requests for interception to be specific, targeted and proportionately circumscribed wherever a person is in the world.

Notification

47. We welcome the proposal in the report that the ISIC should be given the power to inform a subject of an error on the part of the public authority or CSP or to inform the subject of their right to lodge an application to the IPT.[69] The report recommends that this power would be subject to a duty not to disclose anything that would be damaging to national security or prejudice on-going operations. 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 we submitted 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."*[70]

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

[69] Recommendation 99.
[70] 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

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).[71]

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.

Reform of the Investigatory Powers Tribunal

50. We strongly welcome recommendations 114 and 115, which recommend that there should be a right of appeal against rulings of the IPT on points of law and that the IPT should be given the power to make a declaration of incompatibility. We would encourage Members of Parliament to go further and to establish a principle of open proceedings, with the option for the tribunal to determine that closed or partly closed hearings are in the interests of justice.

51. Liberty has long argued for reform of the Investigative Powers Tribunal, the secretive body which hears cases involving state surveillance. 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 and unlike other courts it is unable to make a declaration that legislation is incompatible with the Human Rights Act 1998. This process is arguably a breach of Article 6 of the HRA itself

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

which requires a fair and public hearing, and the right under Article 13 of the ECHR to an effective remedy.

Intelligence and Security Committee

52. The Reviewer recommends that while it continues to be important for a committee of parliamentarians to have oversight of the security and intelligence agencies, it is for Parliament itself to determine whether the ISC is in need of reform (recommendation 120).

53. Liberty strongly encourages Parliamentarians to take the opportunity to reform the Committee. 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."*[72] 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.[73] It later came to light that the security services had been complicit in his ill-treatment. The Joint 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."*[74] The Committee also completely failed to alert Parliament and the public to the scale of mass surveillance being undertaken prior to the Snowden revelations. These repeated derelictions of duty demonstrate that Parliament must reassert its democratic function and undertake reforms necessary to have effective oversight of the use of intrusive powers.

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

[72] Coroner's Inquests into the London bombings of 7 July 2005, paragraph 115.
[73] Joint Committee on Human Rights, Allegations of UK Complicity in Torture, Twenty third report of 2008-2009, paragraphs 60 and 61.
[74] Home Affairs Select Committee Report on Counter-terrorism, Seventeenth report of Session 2013-2014, paragraph 157.

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.[75]

55. Parliament 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.

Conclusion

56. In recommending whole-sale reform of our discredited surveillance regime, the Report represents a significant departure from the Government's repeated claims, since the Snowden revelations of 2013, that the current legislative framework provides effective safeguards to properly protect the privacy of the British people. The report acknowledges the challenges faced by the law enforcement and intelligence agencies, but warns that *"claims of exceptional or unprecedented threat levels – particularly if relied upon for the purposes of curbing well-established liberties – should be approached with scepticism."*[76] Far from accepting the death of privacy as an inevitable by-product of the online communications landscape, the Reviewer makes clear that *"as more of our lives are lived online, and as more and more personal information can be deduced from our electronic footprint, the arguments for strict legal controls on the power of the state become if anything more compelling."*[77]

57. The Reviewer's recommendations are an important first step towards re-building public trust in surveillance conducted with respect for privacy, democracy and the law. As the Report makes clear, both public trust and the co-operation of the private sector demand that judicial warrants replace political authorisation, bringing the UK into line with comparable

[75] See Home Affairs Select Committee Report on Counter-terrorism, Seventeenth report of Session 2013-2014, paragraphs 145-157.
[76] Paragraph 3.6
[77] Paragraph 2.44.

democracies. The Report is clear that the case has not been made for novel communications data retention powers, notwithstanding the repeated claims of Government that a Snoopers' Charter was vital for bridging a gap in capability. In highlighting the concerns of the business community around attempts to impose extra-territorial obligations on service providers, the Reviewer points to the need for the UK Government to take the lead in "developing and negotiating a new international framework for data-sharing among like-minded democratic nations", subject to, where possible, "clearly-defined safeguards". Reform is long overdue and Liberty looks forward to engaging with parliamentarians across the political spectrum to ensure that new surveillance laws maintain those investigative capacities which we genuinely need, whilst providing credible protection for our fundamental freedoms.

Bella Sankey

Rachel Robinson

Sara Ogilvie