LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on Part 6 of the Investigatory Powers Bill for Committee Stage in the House of Commons

April 2016

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

Silkie Carlo
Policy Officer (Technology & Surveillance)
Direct Line: 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

Sam Hawke
Policy Assistant
Direct Line
Email: samuelh@liberty-human-rights.org.uk

Introduction

Liberty welcomes the opportunity to provide briefing and amendments in relation to Part 6 of the Investigatory Powers Bill.

This briefing sets out the following proposals:

- To remove the power for bulk interception of communications (chapter 1)
- To remove the power for bulk acquisition of communications data (chapter 2)
- To remove the power for bulk equipment interference (chapter 3).

Part 6 of the Bill places the breathtakingly broad mass surveillance powers revealed by Edward Snowden and additional bulk surveillance practices on an explicit statutory footing. New powers to intercept, in bulk, 'external' communications (including vast swathes of domestic communications) and to acquire records of the entire nation's communications data are supplemented by powers permitting "industrial scale exploitation" (GCHQ's own words) of electronic devices and networks.

While Liberty supports the use and value of targeted intrusive surveillance powers, we believe that the speculative mass interception of communications; retention and acquisition of communications data; bulk hacking and bulk personal dataset acquisition is unlawful, unnecessary and disproportionate.

A lack of evidence

The Government has not made a serious operational case for bulk surveillance. The bulk powers are presented in the Bill as "*crucial to monitor known and high-priority threats"* and also as "*a vital tool in discovering new targets and identifying emerging threats".*[1] Following criticism by the Joint Committee on the Draft Investigatory Powers Bill, the Home Office was compelled to produce further written evidence to support the case for bulk powers. It also published an 'Operational Case for Bulk Powers' with the publication of the revised Bill on 1 March 2016. However, the documents have provided only a mix of anecdotal and hypothetical evidence. With only vague and limited information provided, it is impossible to assess whether claimed security outcomes could be achieved by using the wealth of targeted and operation-led intrusive surveillance powers at the Agencies' disposal. In nearly all of the examples, references are made to known terrorists, contact with known suspects, visitation to known illegal sites, or a specific "intelligence operation".

[1] Guide to powers, p.20 para. 33

Target development

A former GCHQ intelligence officer provided written evidence to the Joint Committee, at the suggestion of the Head of the Joint Committee's Secretariat, in favour of bulk powers:

> *"The suggestion that UK intelligence agencies work outwards from known targets* instead *of using bulk collection is therefore based on one of two incorrect assumptions: either all the individuals that intelligence agencies require access to have already been identified; or those currently unknown (or subsequently unknown) can all be discovered through analysis of known targets. Unfortunately, the world of intelligence is not that static or predictable."*

However, this appears to be a misrepresentation or misunderstanding of how targeted signals intelligence is conducted. A targeted approach can encompass not only known targets but their social networks; locations known to host illegal activities, online or offline; and geographical locations overseas of specific intelligence interest. Furthermore, signals intelligence is complemented by valuable human intelligence. There is no known case of a terrorist, or any other serious national security threat, being discovered who had no contact with any known suspects or individuals within suspects' zones of suspicion, or who had not accessed extremist, suspect, or illegal materials.

Bulk data failure

A number of former US intelligence professionals have publicly disclosed "bulk data failures" and blown the whistle on mass surveillance practices. William Binney, former Technical Director of the NSA has spoken out about the risk of "bulk data failure" since retiring shortly after the September 11th 2001 attacks when much of the technology he had designed was subverted for mass surveillance. Binney submitted evidence to the Joint Committee on the Draft Bill in which he described the bulk proposals as "*flawed and likely seriously to fail to serve current intelligence and data analysis problems for such purposes as Counter Terrorism".*[2] Binney warned that, "*bulk data over collection from Internet and telephony networks undermines security and has consistently resulted in loss of life in my country and elsewhere, from the 9/11 attacks to date*".

Thomas Drake, a former senior executive at the NSA alongside Binney and later a whistleblower, has also warned of the dangers of mass surveillance programs, both to civil

[2] *Written evidence* – William Binney, 9 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/25753.html

liberties and national security. He has testified[3] that with a "smaller haystack" of data, the 9/11 attacks would have been preventable.[4] FBI whistleblower Coleen Rowley has also warned against mass surveillance systems following the 9/11 intelligence failures she experienced:

> *"I fear that terrorists will succeed in carrying out future attacks – not despite the massive collect-it-all, dragnet approach to intelligence implemented since 9/11, but because of it. This approach has made terrorist activity more difficult to spot and prevent."*[5]

Prior to the Snowden revelations, and in the wake of the murder of Fusilier Lee Rigby, former head of MI5 Dame Stella Rimington warned of the "well-known problem" of big data, drawing comparisons with the East German Stasi's "overdose" of information:

> *"Intelligence services can strangle themselves if they have too much information, because they can't sort out from it what they need to know and what they don't need to know."*[6]

It has been argued, mainly by public officials, that criticisms of big data in intelligence are out-dated. However, whistleblowers and analysts behind the scenes continue to criticise the 'collect it all' approach – most prolifically, Edward Snowden who blew the whistle on mass surveillance practices in 2013 to highlight, "*The problem when you collect it all, when you monitor everyone, you understand nothing".*[7] Previously, (then) US Army Intelligence Analyst Chelsea Manning wrote in private conversation to a confidante, "*approximately 85-90% of global transmissions are sifted through by the NSA… but vast majority is noise… so its getting harder and harder for them to track anything down… its like finding a needle in a haystack",*[8] before blowing the whistle. Furthermore, internal NSA documents shared between analysts, and revealed by Edward Snowden, show continued frustration with data

---

[3] Drake's testimonies to two Congressional investigations about 9/11 remain classified
[4] *After Paris, be careful what you ask for: an interview with Thomas Drake* – Thomas Drake & Mary Fitzgerald, 24 Nov 2015
[5] *The bigger the haystack, the harder the terrorist is to find* – Coleen Rowley, The Guardian, 28 Nov 2014, http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks
[6] *Terror watch lists: Can you keep tabs on every suspect?* – Ruth Alexander, BBC Magazine, 2 June 2013
[7] *Inside NSA, Officials Privately Criticize "Collect It All" Surveillance* – Peter Maas, The Intercept, 28 May 2015, https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/
[8] *Manning-Lamo Chat Logs Revealed* – Wired, 13 July 2011, http://www.wired.com/2011/07/manning-lamo-logs/

overload with titles such as "*The Fallacies Behind the Scenes", "Dealing With a Tsunami of Intercept",* and "*How Can Analysts Deal with the Flood of Collection?*"[9]

In every major terror attack in the Europe and USA since (and including) the 9/11 attack, including the Madrid bombings in 2004, the London 7/7 bombings in 2005, the murder of Lee Rigby in 2013, the Boston bombings in 2013, the January attack on the Charlie Hebdo offices and the Paris attacks in November 2015, some or all of the culprits have been known to the intelligence agencies. The failure to prioritise or action intelligence appropriately is commonly attributed to both human error and pressured resources – these reasons featured in the reports on the London 7/7 bombings[10] and the murder of Lee Rigby.[11]

False positives

Scientists have rightly condemned *"how little of the debate [on mass surveillance] has dealt with the likely success of these tactics (…)",* arguing that *"the efficacy of such surveillance programs must be clearly understood if a rational policy is to be developed"*. The statistics journal *Chance* published a paper on the risk of automatic screening processes (such as those used for bulk interception, bulk data retention and upstream collection), which concluded that whilst a 99% accurate system would indeed report on 99% of the terrorists, the margin of error would also be responsible for producing hundreds of thousands, if not millions, of reports on innocent citizens.[12] This is partly the cause of "bulk data failure" that former intelligence professionals have described. Whilst some argue in favour of bulk powers based on the expectation that developments in technology will somehow make the data valuable one day, as this academic paper shows, even a futuristic, unthinkably accurate processor with only a 1% error margin would produce potentially millions of false positives.

How many terrorist attacks were stopped by bulk access?

Bulk powers have consistently been misrepresented in government rhetoric and Home Office literature as a silver bullet in the fight against terrorism. However, a former Head of GCHQ, Sir David Omand, recently said of bulk powers:

---

[9] *Inside NSA, Officials Privately Criticize "Collect It All" Surveillance* – Peter Maas, The Intercept, 28 May 2015, https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/

[10] *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* – Intelligence and Security Committee, 8 July 2008

[11] *Report on the intelligence relating to the murder of Fusilier Lee Rigby* – Intelligence and Security Committee, 25 Nov 2014

[12] *Until proven guilty: False positives and the war on terror* – Howard Wainer & Sam Savage, Chance, March 2008, 21(1), pp.59-62, https://www.researchgate.net/publication/242713602_Until_proven_guilty_False_positives_and_the_war_on_terror

> *"Don't forget, this is not just about terrorism – that just happens to be something that is on the media mind, on the public mind – this is a much bigger issue about intelligence gathering".*
>
> *"If anyone is tempted to ask the question, how many terrorist attacks were stopped by bulk access, let me just tell you it is a dumb question – it doesn't have a sensible answer".*[13]

No evidence has thus far been provided to illustrate a unique or critical contribution of bulk powers, as opposed to targeted powers, in combatting serious crime or indeed terrorism. Whilst in some cases bulk powers may offer helpful contributions to intelligence gathering, they have not (as far as is publicly known) proved critical in saving lives nor unique in providing intelligence that can be acquired through targeted methods. Furthermore, bulk powers clearly risk burdening intelligence agencies, whose incredible resources may be more effectively directed in targeted surveillance operations.

Are bulk powers proportionate?

It will never be proportionate in a democratic society during peacetime, to mass 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. 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.

The Government has previously attempted to argue that bulk interception is not intrusive if it is carried out by machines rather than humans. This analysis is deeply flawed. There is nothing passive about mechanical State interception of communications and acquisition of communications data. The State cannot physically intercept a communication in a way that does not interfere with privacy just because it claims that human eyes will not necessarily see it.

No protection for confidential communications

[13] Sir David Omand in discussion with NSA whistleblower William Binney: *Does Mass Surveillance Make the World Safer?* Kings College London, 1 Feb 2016

Bulk surveillance also removes the possibility of safeguarding confidential and privileged communications. As a result of proceedings brought by Liberty and others, the IPT disclosed in June 2015 that **GCHQ had unlawfully intercepted and examined** private communications of **the Egyptian Initiative for Personal Rights (EIPR) and Legal Resources Centre (LRC) in South Africa**.[14] It later amended its ruling to clarify that the Agency had unlawfully intercepted and **examined Amnesty International's communications** rather than those of EIPR. GCHQ's activity was however only deemed unlawful because the Agency had breached its own internal guidance in a technical manner. The judgment provided no explanation as to why human rights NGOs had been bulk intercepted and individually examined and perversely did not find this action to amount to a breach of the ECHR. Indeed, the Bill would permit the routine bulk interception and examination of human rights NGOs, lawyers, journalists, elected representatives and others.

Bulk powers, big data

Mass surveillance has significant and untested implications for the future of our society. David Anderson's report noted:

> *"the collection of vast volumes of data enables the identification of patterns and predictions of future behaviour, a process called predictive analytics, data mining or Big Data. An example of this technique is a predictive policing system called PredPol, which analyses large volumes of crime reports to identify areas with high probabilities for certain types of crime. The system has been used by Kent Police to predict when and where drugs crimes and robberies are likely to take place. PredPol is simply about when and where a crime will take place; other technology is aimed at predicting who will commit them. In 2011, the US Department of Homeland Security tested Future Attribute Screening Technology, which seeks to identify potential criminals by monitoring individuals' vital signs, such as cardiovascular signals and respiratory measurements."* [15]

Liberty is concerned that the Agencies and law enforcement will in future seek to exploit so-called Big Data to predict behaviour. This would be a chilling shift in the relationship between the individual and State and could prove disastrous for the life chances of young people belonging to 'suspect' marginalised or disenfranchised groups.

The digital and technological revolution of the past fifteen years has led the Agencies to seek to collect ever-increasing troves of data and to devise mechanical programs to search

[14] The Tribunal did not make determinations concerning whether the other eight organisations had been intercepted.
[15] David Anderson QC, A Question of Trust, paragraph 4.40

databases for so-called suspicious patterns. The current direction is unsustainable. Data is increasing exponentially. Liberty understands the agencies now have the capacity to hoover up 15 times the amount of data being collected when Edward Snowden blew the whistle in 2013. We urge independent parliamentarians and policy makers to reflect on the broader strategy and assess the value of harvesting overwhelming amounts of information.

A golden opportunity

The U.N. Special Rapporteur on the right to privacy recently released a report in which he warned that the proposals in the Investigatory Powers Bill "*prima facie fail the benchmarks set by the ECJ in Schrems and the ECHR in Zakharov".*[16] He urged UK parliamentarians to "*continue, with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimised."* Noting the international effect passing such legislation would have, particularly on the UN member states over which the UK has "*huge influence*", he described the Bill as "*a golden opportunity"* to "*desist from setting a bad example"* by proposing human rights-violating policies.

There is no doubt that these controversial powers are abusive of human rights and threaten our democracy. Furthermore, there is no evidence to support the conjecture that mass surveillance powers are uniquely effective in their stated goals to prevent crime and fight terrorism, or that these goals cannot continue to be pursued with robust targeted surveillance. Given the extraordinary nature of these powers, Liberty believes an independent review into the efficacy of bulk powers is necessary before they receive any further consideration. Furthermore, we urge parliamentarians to consider the ongoing legal challenges to indiscriminate surveillance as legislated for in this Part, including Liberty and other NGOs' legal challenge to mass interception (communicated to the European Court of Human Rights in November 2015) and David Davis MP and Tom Watson MP's challenge to DRIPA, for which the European Court of Justice's ruling is expected this Summer.

[16] *Report of the Special Rapporteur on the right to privacy* – Joseph A. Cannataci, 8 March 2016

Part 6, Chapter 1: Bulk Interception

Amendment

Page 95, line 33, delete clause 119

Page 96, line 43, delete clause 120

Page 97, line 21, delete clause 121

Page 98, line 27, delete clause 122

Page 99, line 1, delete clause 123

Page 99, line 27, delete clause 124

Page 99, line 32, delete clause 125

Page 100, line 9, delete clause 126

Page 100, line 17, delete clause 127

Page 101, line 17, delete clause 128

Page 102, line 30, delete clause 129

Page 103, line 14, delete clause 130

Page 103, line 37, delete clause 131

Page 104, line 25, delete clause 132

Page 106, line 1, delete clause 133

Page 106, line 27, delete clause 134

Page 108, line 4, delete clause 135

Page 108, line 32, delete clause 136

Effect

These amendments would remove the power of the Secretary of State to issue bulk interception warrants (119, 121; 124) and to obtain ‘secondary data’ from bulk interception practices (120).

Therefore, these amendments also remove requirements for warrants affecting overseas operators (122); requirements for a Judicial Commissioner to approve warrants (123); the requirements that must be met for warrants (125), the duration of warrants (126), renewal of warrants (127), modification of warrants (128, 129) and cancellation of warrants (130); and provisions for the implementation of warrants (131). These amendments also remove the restrictions on use (132) and examination (134) of material collected under bulk warrants, as well as disclosure overseas (133), and 'safeguards' for items subject to legal privilege (135), as we firmly believe it is inappropriate to legislate for any collection by mass interception.

Briefing

The intelligence agencies' bulk interception programmes were disclosed for the first time by Edward Snowden in June 2013. They have never been debated or voted for by Parliament. The power to conduct mass interception has instead been inferred by GCHQ from the vaguely worded power in section 8(4) of RIPA. In a radical departure from common and human rights law principles, bulk warrants may be targeted at a telecommunications system or entire populations rather than specific, individual persons or premises as required under section 8(1) RIPA. This approach is maintained in clause 119 of the Bill. Bulk interception results in billions of communications being intercepted each day without any requirement of suspicion or even any discernable link to a particular operation or threat. Liberty understands that the Agencies are currently handling 50 billion communications per day. To place this in context there are only 7 billion people in the world and only 3 billion with access to the internet. The ISC reported that at the end of 2014, there were just 20 section 8(4) warrants in place authorising the vast volume of interception under this power.

Part 6 Chapter 1 provides for the intelligence agencies to conduct bulk interception of "external communications". At first glance, the mass interception these powers permit appears targeted at overseas communications. However, whilst the main purpose of a bulk interception warrant must be to collect "overseas-related" communications or CD, this includes communications where either the sender or recipient is in the UK but their correspondent is not. Internet based communications have further eradicated the distinction between external and internal communications. As first disclosed through Liberty and other NGOs' litigation against the Government,[17] the ISC confirmed that Government considers that an "external communication" occurs every time a UK based person accesses a website

[17] 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#original

located overseas, posts on a social media site overseas such as Facebook, uses overseas cloud storage or uses an overseas email provider such as Hotmail or Gmail. Searches on Google are counted as an external communication. The Joint Committee on the draft Bill reported, "*given the global nature of the internet, the limitation of the bulk powers to 'overseas-related' communications may make little difference in practice to the data that could be gathered under these powers. We recommend that the Government should explain the value of including this language in the Bill".*[18] However, no such explanation has been given.[19]

The Home Office published an 'Operational Case for Bulk Powers' with the publication of the revised Bill on 1 March 2016. The case for bulk interception includes an anecdote about a "*previously unknown individual*" being in contact with "*a Daesh-affiliated extremist in Syria"*.[20] However, this plainly does not justify bulk interception. Robust targeted surveillance of known targets, such as the Daesh-affiliated extremist, should provide for the most efficient and accurate target discovery, such as the discovery of this "*previously unknown individual*". A second anecdote is provided about the discovery that a paedophile, already on the Sex Offenders Register, was accessing illegal sites and paying for images of extreme child sex abuse. Again, robust targeted surveillance of known paedophile networks and known websites hosting illegal content reliably leads to the discovery of new suspects. Neither anecdote justifies the bulk interception of billions of communications of innocent people, but rather supports the case for targeted surveillance.

Material collected under a bulk interception warrant can be examined in accordance with "specified purposes" written into the warrant. The only guidance the Bill provides as to what these purposes may cover is a requirement that it must be more than simply e.g. "the interests of national security", but that "*the purposes may still be general purposes*".[21] Reporting on the draft Bill, the ISC noted that no details had been made available as to what the operational purposes may be, finding it to be, "*completely unsatisfactory: it contradicts the primary purpose of the draft Bill, to provide some much-needed transparency in this area".*[22] The ISC recommended that such detail is published, advising that "*only then can*

[18] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 24
[19] The point is avoided in *Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny,* March 2016, p.52
[20] Supplementary written evidence to the Joint Committee on the draft Investigatory Powers Bill (IPB0165) – Theresa May, December 2015, p.8
[21] Investigatory Powers Bill, clause 125, subsection (4).
[22] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J (ii).

Parliament properly evaluate the provisions of the new legislation in this area"[23] – however, the Government responded by claiming that "*it would be contrary to the interests of national security to publish full details of the Operational Purposes*". Furthermore, the ISC reported that a list of operational purposes had not been finalised, and would not be until after the Bill had passed. Therefore, even if secretly presented with 'examples', the ISC would be: "*unable to provide any reassurance that these 'operational purposes' are appropriate. We fail to see how Parliament is expected to approve any legislation when a key component, on which much of it rests, has not been agreed, let alone scrutinised by an independent body*".[24] The lack of detail around what can amount to "operational purposes" means that the concept offers no practical protection.

While the criteria for selection cannot be "referable to an individual known to be in the British Islands at that time" where "the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual"[25] it is likely that for the vast majority of communications intercepted, the Agencies will have no knowledge as to where the senders and recipients are located. If it later becomes apparent that a target is in the UK (even if they have, in fact, been here all along) that process of selection and examination can continue for 5 days.[26] It seems likely that there will be many cases in which it will be unclear where an individual is currently located. The high threshold of 'knowing' that somebody is in the UK will allow for widespread examination in cases where there is an element of doubt about an individual's current whereabouts. If examination would be in breach of the weak prohibition in clause 134, the relevant agency can apply for a targeted interception warrant to examine the material anyway.[27]

Communications data on people in the UK is acquired, in bulk, as 'secondary data' via bulk interception. As noted by the ISC, "*The RCD* (related communications data) *relating to the communications of people in the UK is unprotected if it is collected via Bulk Interception",* in "*direct contrast"* to the authorisation procedure for public authorities to acquire communications data retained and provided by CSPs. The ISC remarked on this "*simply unacceptable", "inconsistent and largely incomprehensible"* approach and recommended the same authorisation process is applied irrespective of how the data is acquired.[28] However, the Home Office responded that this could "*undermine the operational agility of the*

[23] Ibid.
[24] Ibid.
[25] Investigatory Powers Bill 2016, clause 134, subsection (4).
[26] Investigatory Powers Bill 2016, clause 134, subsection (7).
[27] Investigatory Powers Bill 2016, clause 13.
[28] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; para. 23 and recommendation H

agencies",[29] and the processes proposed in the Bill remain unchanged, allowing the Agencies to use bulk CD outside of the authorisation procedure.

Liberty, along with partner NGOs has lodged a challenge to the practice of mass interception under 8(4) RIPA at the ECtHR. The case was communicated in November 2015. The Joint Committee noted, "***It is possible that bulk interception and equipment interference powers contained in the draft Bill could be exercised in a way that does not comply with the requirements of Article 8 as defined by the Strasbourg court"***.[30] 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 ECtHR ruled that external interception under the pre-RIPA legislation that allowed interception to cover *'such external communications as are described in the warrant'* violated Article 8. The case concerned 'external communications' interception by the Ministry of Defence of Liberty's telephone, fax and email communications between 1990 and 1997 and the violation allowed the interception of almost all external communications transmitted by submarine. The replacement RIPA framework for 'external interception' now subject to challenge is worded almost identically to the power in clause 119 of the Bill.

Therefore, while both the legality and effectiveness of mass interception remains under question, we urge parliamentarians to refrain from committing these powers to statute and to oppose these provisions in the Bill.

[29] *Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny,* March 2016, p.83
[30] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 331

Part 6, Chapter 2: Bulk Acquisition

Amendment

Page 109, line 20, delete clause 138

Page 111, line 1, delete clause 139

Page 111, line 24, delete clause 140

Page 111, line 29, delete clause 141

Page 112, line 5, delete clause 142

Page 112, line 13, delete clause 143

Page 113, line 13, delete clause 144

Page 114, line 20, delete clause 145

Page 115, line 2, delete clause 146

Page 115, line 25, delete clause 147

Page 116, line 7, delete clause 148

Page 116, line 35, delete clause 149

Page 117, line 11, delete clause 150

Page 118, line 39, delete clause 151

Page 119, line 8, delete clause 152

Effect

These amendments would remove the power of the Secretary of State to issue warrants to acquire bulk communications data (138, 140).

Therefore, these amendments also remove the requirements for Judicial Commissioners to approve bulk acquisition warrants (139); the requirements that must be met by warrants (141); their duration (142), renewal (143), modification (144, 145), cancellation (146) and implementation (147). These amendments also remove requirements relating to the service of warrants outside the UK (148), the duty of operators to comply with bulk warrants (149).

Furthermore, they remove restrictions (150) and the offence (152) of disclosing data obtained under a bulk acquisition warrant (150) and 'safeguards' relating to examination of the data (151), as we firmly believe it is inappropriate to legislate for any mass acquisition of communications data.

Briefing

On the day that the draft Bill was published, the Home Secretary announced that the Agencies have been acquiring the communications data of the UK population in bulk under the vaguely worded section 94 of the *Telecommunications Act 1984* since 2005.[31] This had never previously been publicly admitted by the Executive and was apparently only known by a handful of Cabinet ministers.[32] Parliamentarians had previously been led to believe that communications data retention and acquisition by the Agencies took place under RIPA and DRIPA as the legislation specifically permits the Agencies to acquire communications data on national security and serious crime grounds.

By contrast with bulk interception, where a half-hearted attempt is made to tie surveillance to "overseas" communications, acquisition has as its main purpose the acquisition of data held by UK based companies. The power also purports to have extraterritorial effect.

Communications data provides a detailed and revealing picture of somebody's life in the digital age. As defined under DRIPA and RIPA it can disclose the date, time, duration and type of communication, the type of communication equipment used, its location, the calling telephone number and the receiving telephone number. This can reveal personal and sensitive information about an individual's relationships, habits, preferences, political views, medical concerns and the streets they walk. As the CJEU has put it:

> *"those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*[33]

---

[31] Secretary of State for the Home Office the Right Honourable Theresa May, Oral Statement on publication of the Draft Investigatory Powers Bill, 4 November 2015 - https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

[32] http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

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

In December 2013, US District of Colombia Judge Richard J Leon found that a lawsuit challenging the NSA's previous regime of bulk metadata collection demonstrated a "substantial likelihood of success"[34] and said of modern data metadata:

> *"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 Amendment."*

As communications have become increasingly digital, the data generated is much more revealing and copious than before, allowing the state to put together a complete and rich picture of what a person does, thinks, with whom, when and where. Often, communications data can be of more use than content: it is expansive, easy to handle, analyse and filter; and, it tends to be collected in a consistent manner. In 2015 the ISC remarked: *"We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications."*[35]

The value of metadata and the use that the UK's closest ally is prepared to make of it was left beyond doubt following comments by the former head of the NSA, Michael Hayden in 2014: "*We kill people based on metadata*."[36]

Furthermore, there are many situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a reporter on a national newspaper immediately before a major whistleblower scandal fills the front pages; the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody.

In its supplementary written evidence to the Joint Committee, the Home Office makes the case for the retention of bulk communications data by providing four anecdotes about counter-terrorism operations. Working outwards from known targets or an intelligence lead,

---

[34] 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-judgerules-nsa-program-is-likely-unconstitutional/668/.

[35] *Privacy and Security: a modern and transparent legal framework* - Intelligence and Security Committee, March 2015, paragraph 80.

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

the security and intelligence agencies were able to identify new targets and uncover plots. However, a targeted approach to communications data retention works by exactly the same process, without the need for retaining the communications data of many millions of people. The security and intelligence agencies should retain only the communications data of known targets and individuals within their social network (usually, to two 'hops').

The available evidence indicates that mass surveillance powers have not been effective in tackling serious crime, especially not terrorism. Rather, there is evidence that mass surveillance practices impede law enforcement efforts. Bulk telephone data has not proved useful for counterterrorism in the U.S.. The Privacy and Civil Liberties Oversight Board, an independent executive branch board in the U.S., found that the bulk telephone records program conducted under Section 215 of the USA Patriot Act not only raised constitutional and legal concerns, but had no material counterterrorism value:

> *"Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."*[37]

Similarly, the President's Review Group on Intelligence and Communications Technologies concluded in 2013:

> *"Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."*[38]

Both panels' findings refuted Keith Alexander and President Obama's claims that "at least fifty threats" had been averted and "lives have been saved" as a result of bulk metadata retention. Both panels advised that the bulk surveillance program should be shut down. Section 215 was allowed to expire in May 2015.[39] The USA Freedom Act followed, reducing the capacity of the NSA to undertake mass collection of Americans' phone records, requiring

---

[37] *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* – Privacy and Civil Liberties Oversight Board, 23 Jan 2014, p.11

[38] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* – 12 Dec 2013, p. 104

[39] *Section 215 Expires – For Now* – Mark Jaycox & Dia Kayyali, EFF, 31 May 2015

instead that a subset of data be requested pursuant to limits set out in the Act.[40] However, in the UK, our Government is proposing not only bulk phone data retention and acquisition, but communications data from email, messaging, VoIP (Skype, etc.), app use, web browsing, and all other internet connections. This is vastly disproportionate, evidently ineffective, and out of sync with the international precedent. The Home Office has resisted commissioning independent reviews, similar to those in the US, to evaluate the efficacy of bulk programmes. **However**, **such reviews should be considered a bare minimum to justify proposals before they are scrutinised by Parliament and considered for compatibility with human rights law.**

The bulk acquisition and automated analysis of communications data is an extraordinary power which could be used for profiling and pattern analysis at the population level. This highly controversial power must be assessed for effectiveness by independent reviewers and for legality by the courts before it is considered any further.

[40] USA Freedom Act 2015, available at: http://judiciary.house.gov/_cache/files/1cb59778-0a72-4c09-920d-0e22bf692bb4/fisa-01-xml.pdf.

Part 6, Chapter 3: Bulk Equipment Interference

Amendment

Page 120, line 10, delete clause 154

Page 121, line 33, delete clause 155

Page 122, line 4, delete clause 156

Page 123, line 1, delete clause 157

Page 123, line 24, delete clause 158

Page 123, line 41, delete clause 159

Page 124, line 34, delete clause 160

Page 125, line 3, delete clause 161

Page 125, line 25, delete clause 162

Page 126, line 3, delete clause 163

Page 127, line 1, delete clause 164

Page 128, line 11, delete clause 165

Page 129, line 1, delete clause 166

Page 129, line 25, delete clause 167

Page 130, line 14, delete clause 168

Page 131, line 33, delete clause 169

Page 132, line 4, delete clause 170

Page 133, line 30, delete clause 171

Page 134, line 12, delete clause 172

Effect

These amendments would remove the power of the Secretary of State to issue bulk equipment interference warrants (154, 156, 160)

Therefore, these amendments would also remove the requirement for Judicial Commissioners to approve bulk hacking warrants (157), remove provisions for 'urgent' bulk hacking warrants (158, 159), and remove the broad separate category of unprotected 'equipment data' (155). These amendments would also remove the requirements that must be met for bulk hacking warrants (161), and provisions for their duration (162), renewal (163), modification (164, 165), cancellation (166), and implementation (167). These amendments would also remove clauses relating to the restrictions on the use (168, 172) and examination (170) of material obtained under bulk hacking warrants, including for overseas disclosure (169) and for items subject to legal privilege (171), as Liberty believes it is never appropriate to conduct bulk equipment interference or gain any material via this method.

Briefing

The use of targeted hacking by the Agencies was only very recently acknowledged by Government through the publication by the Home Office of an Equipment Interference Code of Practice although it made no mention of bulk hacking capabilities. The scope of a bulk equipment interference warrant under the Bill is astonishingly broad, paving the way for intrusions over and above those revealed by Snowden, pinpointing hacking as the modus operandi of our expanding surveillance state. As with bulk interception, the main (but not sole) aim of the warrant must be to facilitate the obtaining of overseas data, but this does not prevent data on UK residents being collected as a subsidiary objective, or in pursuit of the main aim.[41] A bulk hacking warrant can authorise interference with any equipment whatsoever, for the purposes of obtaining communications, equipment data or "*information"*.[42] Bulk warrants can be issued in the interests of national security, economic wellbeing, or for the prevention and detection of serious crime.[43]

The Home Office says that "*bulk equipment interference*" has been practiced under the Intelligence Services Act 1994,[44] which allows for interference with property or "wireless

[41] Investigatory Powers Bill 2016*,* clause 154, subsection (1)(c)
[42] Ibid*.*
[43] Investigatory Powers Bill 2016*,* clause 156
[44] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* pp.20-21

telegraphy".[45] Under this law, intelligence services can acquire a warrant to search a property or intercept a person's phone calls. There is no mention in the Act of bulk or mass equipment interference. However, under these out-dated Acts, British intelligence agencies have conducted intrusive, destructive and disturbing mass hacks, such as hacking the largest SIM manufacturer in the world to enable interception of millions of users' calls.[46] The Intelligence Services Act 1994 was written prior to the technological revolution of the past twenty years and cannot be considered a lawful basis for the mass hacking of technologies that were not even conceivable at the time of the Act's writing. Indeed, the Snowden documents revealed that British intelligence agencies expressed concern that their mass hacking practices "*may be illegal.*"[47] [48]

Bulk hacking - a significant expansion of power

The "Guide to powers" accompanying the draft Bill made clear that bulk hacking is a significant step beyond conventional and surveillance powers, remarking that bulk equipment interference "*is used increasingly to mitigate the inability to acquire intelligence through conventional bulk interception and to access data from computers which may never otherwise have been obtainable" (emphasis added).*[49] Labelling mass interception powers as "conventional" when it is this Bill that for the very first time avows them makes a mockery of our parliamentary democracy. It also demonstrates the apparently insatiable demand from the security services to have unbridled access to all information. This is particularly concerning in light of the broad definition of 'equipment' in the Bill. The Bill defines "*equipment"* as "*equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment*"[50]. This is unfathomably open-ended and could even include cars and aircraft, leaving the power open to potential abuses not just by future UK governments, buy by other states that will follow our lead in legislation.

Following scrutiny of the draft Bill, the ISC reported that "***the Committee has not been provided with sufficient compelling evidence as to why the Agencies require Bulk Equipment Interference warrants"*** and "***therefore recommends that Bulk Equipment***

[45] Intelligence Services Act 1994*,* Section 5
[46] *The Great SIM Heist* – Jeremy Scahill & Josh Begley, The Intercept, 19 Feb 2015
[47] *UK Perspective on MIKEY-IBAKE*, Sept 2010, p.3 (https://www.documentcloud.org/documents/1077367-uk-perspective-on-mikey-ibake.html)
[48] As recently as April 2013, GCHQ was reluctant to extend deployment of QUANTUM malware due to "legal/policy restrictions": *Legal Issues UK Regarding Sweden and Quantum,* (https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html)
[49] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* pp.20-21
[50] Investigatory Powers Bill 2016*,* clause 173, subsection (1).

Interference warrants are removed from the new legislation"[51]*.* However, this unjustified power remains in the revised Bill against the ISC's recommendation. In fact, in response to the ISC's recommendation, the Home Office admitted that "*the Secretary of State is not able to fully assess at the time of issuing the warrant the necessity and proportionality of each interference".*[52]

Bulk hacking - Indiscriminate and speculative

Bulk hacking is by its nature indiscriminate, as acknowledged by the Draft Bill's Explanatory Notes: "*bulk equipment interference is not targeted against particular person(s), organisation(s) or location(s) or against equipment that is being used for particular activities".*[53] Instead, systems, services and software that have been carefully constructed to provide security are intentionally corrupted to impose the eyes and ears of the intelligence agencies on every phone call, text message and web click. In the offline world, granting this power would mean allowing secret services to break into and bug every house, leaving broken windows[54] for anyone else to get in but all without the individual whose house it is knowing this has happened. In the digital world, even more rich and revealing data can be gathered as computers and mobile devices have taken the place of our filing cabinets, diaries, calendars, video archives, photo albums, book shelves, address books and correspondence files. Furthermore, this digital forced entry does not only entail intrusion into highly personal spaces, but control over them. For example, spies can alter, add or delete files, send messages, turn devices on or off, or covertly activate cameras and microphones. As demonstrated by GCHQ's OPTIC NERVE program,[55] this could literally mean subverting millions of webcams into covert home surveillance cameras. Such extraordinary power over the private lives of citizens fundamentally alters the relationship between citizen and state, and will breed distrust in law enforcement while having potentially significant repercussions for the Rule of Law. In human rights terms, such sweeping and speculative powers can never meet a test of necessity and proportionality.

---

[51] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation D

[52] *Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny,* March 2016, p.80

[53] *Draft Investigatory Powers Bill 2015: Explanatory Notes*, p. 83

[54] A US intelligence official described state hacking using a similar analogy: *"You pry open the window somewhere and leave it so when you come back the owner doesn't know its unlocked, but you can get back in when you want to".* Quoted in, *U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show* – Barton Gellman & Ellen Nakashima, 30 Aug 2013

[55] In which several millions of Yahoo users' webcam calls were intercepted to take and store images for a facial recognition program. *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ* – Spencer Ackerman & James Ball, The Guardian, 28 Feb 2014 (http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo).

Security repercussions of bulk hacking

Bulk hacking critically damages the security of complex modern technologies upon which modern society is built. The Five Eyes intelligence agencies find security flaws in software and stockpile them for later 'equipment interference', rather than inform developers so that they can be fixed or responsibly dealt with.[56]As such, mass hacking goals prevent intelligence agencies from protecting the public's cybersecurity. President Obama's Review Group of Intelligence and Communications Technologies criticised this approach, concluding: "*In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities – 'patching' them – strengthens the security of US Government, critical infrastructure, and other computer systems."*[57] Furthermore, the UN Group of Governmental Experts (UN GGE) recently released a consensus report, recommending that states "*should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions*".[58] Although the alarm has been raised on the danger of stockpiling exploits, this Bill would proliferate the practice and in fact boost the market for exploits to be created and sold. In addition, security vulnerabilities created or stockpiled by British intelligence agencies can also be exploited by foreign intelligence agencies or any non-state actors who discover them. An explicit British bulk hacking law will set a disturbing precedent for other, more authoritarian states to follow and join a cyber-arms race.

"*Bulk equipment interference"* is an especially excessive, dangerous and destructive power. Bulk hacking is one of the most objectionable powers in the Bill, jeopardising human rights in the present and future. We urge parliamentarians to follow the ISC's advice and remove powers for bulk equipment interference from the Bill.

Silkie Carlo

[56] *Mind-blowing secrets of NSA's security exploit stockpile revealed at last* – Shaun Nichols, The Register, 4 Sept 2015
[57] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* 12 Dec 2013, p. 220
[58] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – UN GGE, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174