LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on Part 9 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 9, 'Miscellaneous and general provisions', of the Investigatory Powers Bill.

This briefing sets out the following proposals:

- To remove the power to issue national security notices
- To remove the power to issue technical capability notices

National security notices and technical capability notices provide exceedingly broad powers to oblige telecommunications operators either within or outside the UK to comply with any obligations imposed by the Secretary of State, including the removal of electronic protection. This provision is understood to allow the highly controversial practice of forcing operators to covertly remove encryption from their communications products and services.

Security and encryption

Encryption is now a widely used standard to protect the ever-expanding uses of communications technologies in an increasingly hostile digital environment: from mobile phones and smart phones to personal hard drives, online banking and e-commerce, critical infrastructures, transport networks, institutional and business computer networks, cloud storage, emailing and messaging, web browsing and online shopping. The renewed and extended assault on encryption in the Bill demonstrates a misguided commitment on the part of the State to undermine secure spaces in the furtherance of mass surveillance ambitions. The Government's coercion of telecommunications operators to maintain covert interception capabilities would force products and services to be designed with the required insecurity built-in.

Meanwhile, anyone intent on evading surveillance need not rely on a telecommunications service to provide encryption, but can easily use open source encryption software with personally generated and managed keys. This type of client-side encryption, typically used to encrypt files and email communications, is independent of third party providers, and as such would remain unaffected by this legislation.

Undermining encryption provided by telecommunications operators, however, seriously jeopardises the security of technologies, their users, and modern digital society as a whole. As the Government's Reviewer, David Anderson, found:

> *"Few now contend for a master key to all communications held by the state, for a requirement to hold data locally in unencrypted form, or for a guaranteed facility to*

> *insert back doors into any telecommunications system. Such tools threaten the integrity of our communications and of the internet itself."*[1]

However, these practices would indeed be the consequence of clause 217 in the Bill. The Information Technology Industry Council (ITI), which represents 62 of the largest technology companies worldwide including Apple, Microsoft, Google, Samsung, Twitter, and Facebook released a statement following the publication of the draft Bill in defence of encryption:

> *Encryption is a security tool we rely on every day to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to otherwise preserve our security and safety. We deeply appreciate law enforcement's and the national security community's work to protect us, but weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy.*[2]

In a recent research paper by world leading technologists, it was concluded that US and UK governments' proposals to achieve "exceptional access" to encrypted communications would "*raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm".*[3] Security experts agree. In a recent op-ed for the Washington Post Mike McConnell, the former Director of the NSA, Michael Chertoff, former Secretary of Homeland Security and William Lynn, the former Deputy Secretary of Defence argued that, in order to protect economic and national security, encryption should not be undermined for Government surveillance. They concluded, "*(w)e believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring*".[4]

Apple's Chief Executive Tim Cook has argued against government attempts to 'backdoor' (i.e. seek or create vulnerabilities in software to achieve unauthorised access) encryption, explaining, *"(t)o protect people who use any products, you have to encrypt (…) Any*

---

[1] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, paragraph 13.12, p.248
[2] *Tech Responds to Calls to Weaken Encryption* – Information Technology Council, 19 Nov 2015
[3] *Keys Under Doormats* – H. Abelson, R. Anderson, S. M. Bellovin, et al., MIT, 7 July 2015
[4] *Why the fear over ubiquitous data encryption is overblown* – Mike McConnell, Michael Chertoff & William Lynn, The Washington Post, 28 July 2015

backdoor is a backdoor for everyone (…) Opening a backdoor can have very dire consequences"[5].

The UK's national cybersecurity, identified as a tier-one risk in the recent Strategic Defence and Security Review, is an increasingly critical element of our national security that *"underpin(s) many of the other risks we face".*[6] As stated by the Information Technology Council, "*weakening security with the aim of advancing security simply does not make sense".*[7]

In addition, the Software and Information Industry Association (SIIA) submitted written evidence to the Science and Technology Select Committee regarding the Draft Bill, seeking clarification on provisions relating to encryption, and expressing concerns about the pressure to respond to similar requests from multiple governments:

> *Should Western democracies require "backdoors," companies will not have a credible reason not to provide backdoors to other countries. This increases the exposure of critical infrastructure and individuals to attacks and spying from nation state actors, as well as from terrorists and criminals.* [8]

The free software community Mozilla, whose web browser 'Firefox' encrypts 100 billion individual web data transfers every day, also submitted written evidence expressing the same concern.[9]

Human rights and encryption

Encryption is a critical tool for protecting individuals' rights to privacy and freedom of expression – particularly for those in sensitive professions, and discriminated and minority groups. In a 2015 report, David Kaye, the United Nations Special Rapporteur on Freedom of Expression, described encryption as a leading vehicle for online security and freedom, giving individuals:

> *"a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organisations, members of ethnic or religious groups, those persecuted*

---

[5] *Apple's Tim Cook declares the end of the PC and hints at new medical product* – Allister Heath, The Telegraph, 10 Nov 2015
[6] SDSR, Annex A, paragraph 4: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
[7] *Tech Responds to Calls to Weaken Encryption* – Information Technology Council, 19 Nov 2015
[8] *Written evidence regarding Investigatory Powers Bill* - Software & Information Industry Association, 1 Dec 2015
[9] *Written evidence regarding Investigatory Powers Bill* - Mozilla, 1 Dec 2015

> *because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."*[10]

In addition to protecting freedom of expression, Kaye found encryption "*essential"* for the exercise of further vital rights, including "*economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity"*[11]*.* Kaye analysed submissions on the laws and policies of member states as well as submissions from civil society groups, leading him to conclude:

> *"States should not restrict encryption (…) which facilitate(s) and often enable(s) the rights to freedom of opinion and expression* (…) *States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows"*[12]

There is increasing awareness in the US of the dangers of undermining encryption for mass surveillance purposes. A recent draft opinion paper on strategic approaches to encryption from the National Security Council argued that "*(o)verall, the benefits to privacy, civil liberties and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption*". The NSC concluded, "*the Administration will not seek legislation that compels providers to enable government access to encrypted information, even pursuant to lawful process*"[13].

British business and encryption

"*The voice of the internet industry"*, the Internet Service Providers Association (ISPA) expressed concern that "*attempts to undermine encryption could damage user trust in online services*".[14] Indeed, if the provision to force removal of encryption is passed it is very likely that users – particularly those in sensitive sectors such as law, journalism and health - will move away from UK technologies and towards providers based in countries that do not undermine security, thus damaging the UK's digital economy. Furthermore, some UK providers may have to discontinue services if they do not wish to mislead customers as to

---

[10] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* – UN Human Rights Council, 22 May 2015, paragraph 1
[11] Ibid, paragraph 56
[12] Ibid, paragraph 60. Note: a key escrow is an arrangement in which cryptographic keys are entrusted to a third party (in this context, the state).
[13] *Review of Strategic Approaches* – National Security Council; cited in *Obama faces growing momentum to support widespread encryption* - Ellen Nakashima & Andrea Peterson, The Washington Post, 16 Sept 2015
[14] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015

the security features or if their product design does not include a mechanism by which to remove users' encryption.

Recommendation

- Liberty is calling for a formal definition of 'national security' in law. Until such time, such an enabling provision as open-ended 'national security notices' cannot be properly assessed. **In the absence of a definition of 'national security' Liberty believes clause 216 should be removed from the Bill.**

- Liberty believes the power to force the removal of, or in any way undermine, encryption over entire communication services could indiscriminately deny millions of people the right to privacy, and jeopardise freedom of expression. Therefore, **Liberty believes clause 217 should be removed from the Bill.**

- We concur with David Anderson's view that *"(f)ar preferable, on any view, is **a law-based system in which encryption keys are handed over (…)** only after properly authorised requests*".[15] This should be a tightly regulated power **subject to judicial authorisation, and exercised only in the interests of investigating serious crimes**. Anderson argued that the best way to set an example to other nations, thus protecting international cybersecurity, is "*by demonstrating an ability to patrol those spaces in tightly defined circumstances, and with sufficient safeguards against abuse*".[16]

[15] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, paragraph 13.12, p.248
[16] Ibid. Paragraph 13.14, p.248

Amendment: to remove national security notices

Page 166, line 35, delete clause 216

Effect

This amendment would remove the provision for national security notices.

Briefing

National security notices provide a blank-cheque power in the Bill, requiring a telecommunications operator to 'carry out any conduct' for the purposes of 'facilitating anything done by an intelligence service under any enactment other than this Act'. As such, it provides a power to force a telecommunications operator to engage in *any* conduct the Secretary of State demands - that is not otherwise provided for in the Bill. There is no judicial authorisation required to issue such a notice. The recipient of such a notice must comply with it[17] but must not disclose the existence or contents of it.[18] Without the ability to foresee the kind of activity and intrusion such obligations could entail – particularly whilst 'national security' remains undefined - it is impossible to condone this power.

Amendment: to remove technical capability notices

Page 167, line 19, delete clause 217

Effect

This amendment would remove the provision for technical capability notices.

Briefing

Clause 217 has proved to be one of the most controversial clauses in the Bill, and one of the most concerning for telecommunications companies and the tech sector both within the UK and abroad. The Intelligence and Security Committee acknowledged communications service providers' '*serious concern as to this seemingly open-ended and unconstrained power*'.[19]

Similar to 'national security notices' in clause 216, 'technical capability notices' provide the Government with a blank-cheque power to force telecommunications operators to comply

[17] Investigatory Powers Bill 2016, clause 218, subsection (9)
[18] Investigatory Powers Bill 2016, clause 218, subsection (8)
[19] Report of the Intelligence and Security Committee on the Draft Investigatory Powers Bill, para. J (x), page 12

with ‘any applicable obligations specified in the notice’.[20] The recipient of such a notice must comply with it[21] but must not disclose the existence or contents of it.[22] Thus, were an Apple v FBI scenario to occur in the UK, Apple would not be able to disclose even the fact that it had been served with a notice, let alone challenge it in court.

Furthermore, the issuance of such a notice does not require prior judicial authorisation or an objective test of necessity and proportionality. Submissions to the Joint Committee scrutinising the Draft Bill from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc. and Virgin Media questioned why these notices were not subject to judicial authorisation before being served on communications service providers.[23] It means that the specific risks and technical consequences that removal of electronic protections and other measures to maintain interception capabilities incur may not be sufficiently accounted for – at least not by any neutral body[24] - before notices are issued.

It is of further concern that obligations under clause 217 may not necessarily relate to an existing warrant or authorisation. Therefore, a service provider could be compelled with obligations to remove encryption and security measures, perhaps with a view to seeking a warrant for interception in the future, but not necessarily currently holding that warrant. Therefore, when a warrant for further surveillance is applied for, it is unlikely that the forced removal of encryption or security measures would form part of the proportionality assessment, as it could already have taken place.

The proposal to force telecommunications operators to allow government access to masses of encrypted communications, by an offline analogy, is akin to forcing every locksmith to retain duplicates or a master key to thousands of houses to enable suspicionless property searches. By any usual test, this would not be considered a necessary or proportionate measure.

[20] Investigatory Powers Bill 2016*,* clause 217, subsection (1)(a)
[21] Investigatory Powers Bill 2016*,* clause 218, subsection (9)
[22] Investigatory Powers Bill 2016*,* clause 218, subsection (8)
[23] Written evidence from Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc. and Yahoo Inc (IPB0116) and Virgin Media (IPB0160)
[24] The Secretary of State must only ‘consult’ the Technical Advisory Board, a board consisting of six telecommunication company representatives and six intelligence agency representatives, and persons subject to the notice.

Consequential amendments following deletion of national security and technical capability notices

Page 168, line 31, delete clause 218

Page 169, line 38, delete clause 219

Page 170, line 18, delete clause 220

Silkie Carlo