PRIVACY INTERNATIONAL

Submitted to the Honourable Members of the Science & Technology Committee of the House of Commons

Submission to the Science and Technology Committee

Submitted by Privacy International

27 November 2015

PRIVACY INTERNATIONAL SUBMISSION IN RESPONSE TO SCIENCE & TECHNOLOGY COMMITTEE CALL FOR EVIDENCE ON THE DRAFT INVESTIGATORY POWERS BILL

27 NOVEMBER 2015

Submitted to the Honourable Members of the Science & Technology Committee of the House of Commons:

Introduction

1. Thank you for the opportunity to provide comments on the draft Investigatory Powers Bill (IP Bill). Increasingly, the internet plays a central role in the lives of people globally. For some, the internet provides community, and offers like-minded people a space to discuss and share ideas and thoughts. For others, the internet gives the ability to speak out against dictatorial governments and demand change and social progress. The internet fosters creative and intellectual growth, and allows individuals to carve out a niche, and explore and express who they are with the world. Trust in the security and democratic nature of the internet has shaped how it is used today.

2. Privacy International was founded in 1990. It is a leading charity organisation promoting the right to privacy across the world. It is based in London and, within its range of activities, focuses on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development and the United Nations.

3. The draft IP Bill introduced by Home Secretary Theresa May on November 4, 2015, aims to overhaul existing surveillance legislation and act as an example of the "gold standard" of surveillance legislation for governments around the world. Unfortunately, it falls short of this goal. In its current form, the IP Bill attempts to legitimise and expand upon surveillance powers currently held by British intelligence and police agencies. Privacy International is deeply concerned by the extent of these powers, and the vague and obscure nature of the language in which some of them are articulated.

4. As requested by the Committee, in this submission we focus on how the IP Bill in its current form would impact British and global communications service providers, related business, and consumers of Information Communications Technologies. Three aspects of the IP Bill cause us particular concern in this regard: (1) its provision for equipment interference, especially when used in bulk or against communications infrastructure; (2) the obligations it places on communication service providers (CSPs) to fundamentally weaken their systems in order to give access to intelligence and police agencies; and (3) the requirement that CSPs must collect and retain personal customer data for up to 12 months, even if that data would not normally be retained in the CSPs' course of business. All three impact negatively on the privacy and security of global communications services and those who use them.

Definitions

5. Throughout this submission, the word "computer" refers to any device connected to the internet, and is not limited to laptops, desktops, and mobile phones. We use the term to include, but not be limited to, Smart Technologies such as Wi-Fi-enabled thermostats, smoke

detectors, and security systems, watches, fitness wrist bands, smart televisions, smart cars, and more. It also refers to the servers and networking equipment that form the basis of most communications service providers' businesses.[1]

6. Additionally, the IP Bill refers to communications service providers variously as "telecommunication services"[2], "telecommunication systems"[3], and "telecommunications operators"[4]. While the distinctions between these definitions are important, and not always clear, for the sake of brevity in this submission we will refer to collective to the companies encompassed by these definitions as communications service providers.

The impact on communications service providers and related businesses, and the consequences for individuals

7. If implemented in its current form, the draft IP Bill would require communications service providers to fundamentally weaken the security of their systems, which may cause them to question whether to continue doing business with and in the United Kingdom. The ramifications would be felt not only within the technology sector, but also within related businesses that rely on secure communications and customer trust. Many of these businesses contribute greatly to the British economy, and include the banking, financial, and legal sector, as well as the computer software, hardware, anti-virus, gaming, and start-up industries.

8. Individuals will consequently face a reduction in their privacy and security, which could undermine trust in the entire communications system. The internet offers a democratic space in which personal exploration, growth, change, and development is possible, and without trust in the systems that enable such exploration, such positive growth is curtailed.

9. Privacy International outlines below key ways in which the draft IP Bill would weaken the services of communications service providers and related businesses, as well as the impact on the security and privacy of all of our communications.

Equipment Interference

10. For the first time in the UK, the draft IP Bill includes statutory provisions describing the power of law enforcement and the intelligence services to hack into our computers. This power is called "Equipment Interference", and is detailed in Part 5 and, as a "bulk" power, in Part 6, Chapter 3. Hacking, as undertaken by any actor, including the state, fundamentally impacts on the security of computers and the internet. It incentivises the state to maintain security vulnerabilities that allow any attacker – whether GCHQ, another country's intelligence agency or a cyber criminal – potential access to our devices. When deployed against networks or in "bulk", hacking can undermine the security of all our communications, including those that form the core of financial transactions. These security concerns affect all communications service providers and the consumers who use their services.

11. When an agent takes control of a computer by hacking it, there are few limits on what can be done. Unlike intercept capabilities, hacking capabilities can be deployed in any number

1 The IP Bill contains, in the sections related to equipment interference, a definition of 'equipment' as 'equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment" (Clauses 105 and 149.)
2 Clause 193(11), Part 9, Chapter 2, Investigatory Powers Bill
3 Clause 193(13), Part 9, Chapter 2, Investigatory Powers Bill
4 Clause 193(10), Part 9, Chapter 2, Investigatory Powers Bill

of configurations to do any number of different things. The logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies and the police to conduct real-time surveillance, while access to stored data enables analysis of a user's movements for a lengthy period prior to the search, access to save documents and notes, draft messages and emails, and more.

12. For an increasing number of people, personal digital devices contain the most private information they store anywhere. Computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, and correspondence. They are also slowly replacing our formal identification documents, and our bank and credit cards. They hold information that may never have been set down or communicated elsewhere. Whatever information is stored on our computers and mobile phones becomes immediately obtainable with hacking. From text messages, emails and phone records, to address books, notes and calendars, as one GCHQ document explains, "if it's on the phone, we can get it."[5]

13. Hacking is not a passive form of surveillance. It can be employed to corrupt a target computer's files, to plant or delete documents or data on that computer remotely, or to send fake communications from the computer. When deployed against servers or networks, the potential for manipulation and resulting damage becomes even greater.

14. Hacking is most often carried out by remotely accessing the target computer. This can be done in a variety of ways such as sending out malicious emails that install malware when the email recipient clicks on a link or opens a file contained in the email[6] or using preexisting vulnerabilities in computer systems to install malware without the affirmative participation of the user.[7]

15. Using this latter mechanism, hacking by its nature exploits weaknesses in software and hardware that is often used by millions of people. One US intelligence official analogised using hacking to a situation in which "[y]ou pry open the window somewhere and leave it so when you come back the owner doesn't know it's unlocked, but you can get back in when you want to."[8] This weakening of systems leads to sacrificing the security of the communications that we all rely on for banking, commerce and other everyday transactions in the name of access for intelligence agencies. One example of how this occurs is the stockpiling of zero days.

16. *Stockpiling of zero days:* Intelligence agencies and police use a variety of methods to exploit hardware and software. Many of those methods rely on the use of a vulnerability – a pre-existing error, often called a "bug", in hardware or software that allows it to be used in a

---

5 Capability - iPhone (28 January 2014) [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data#img-3 [Accessed 26 November 2015]

6 Malware is a malicious software, designed to intrude or have other effects unwanted to the owner or user of the computer.

7 For further background on hacking, please see Privacy International's submission on the Equipment Interference Code of Practice (20 March 2015) Available from: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf

8 Gellman, B. and Nakashima, E. (30 August 2013) U.S. spy agencies mounted 231 offensive cyber- operations in 2011, documents show, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html [Accessed 26 November 2015]

manner that was not intended or anticipated. Zero day vulnerabilities get their name from the fact that, when identified, the computer user has had "zero days" to fix them before attackers can exploit the vulnerability. In the normal course, when researchers and others discover vulnerabilities, they report the vulnerability to the company responsible for the security of the equipment affected. If a vulnerability is discovered by intelligence agencies or law enforcement, however, they have conflicting incentives. On the one hand, they could keep it secret it in order to use it offensively as part of a hacking attack, or to stockpile it for future use. On the other hand, they could reveal it for the public good so that it can be fixed.

17. By using zero days offensively as part of attacks, British intelligence and police agencies are preventing potentially millions of individuals and companies from being protected. Such zero day vulnerabilities could be used not only to target personal computers and phones, but also other devices connected to the internet, such as smart watches, fitness bands, smart cars, and more. This perverse situation has drawn criticism from the US President's own Review Group on Intelligence and Communications Technologies. When considering the zero day problem, they recommended that "[i]n 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."[9]

18. For all of these reasons, we question whether hacking can ever be a legitimate for a state surveillance. If it to be used, it must be in only the most narrowly defined circumstances with the strictest safeguards. The IP Bill fails to provide these. Instead, Part 5, the supposedly "targeted" hacking provision, permits attacks on broad categories of equipment that could include that belonging to communications service providers.[10] Part 6, Chapter 3 of the Bill compounds this problem by allowing hacking to be carried out "in bulk" when it is directed overseas. This "bulk" provision gives almost unfettered powers to the intelligence services to decide who and when to hack.

19. In this context of broad powers and insufficient safeguards, there is nothing in the IP Bill that would prevent the hacking of communications networks or the servers of communications service providers like Google and Microsoft. Indeed, an earlier published draft Equipment Interference Code of Practice specifically reserves the power of the intelligence services to hack "individuals who are not intelligence targets in their own right."[11]

20. In addition, the draft IP Bill would make communications service providers complicit in the police and intelligence services' hacking activities. Clause 99 requires any person (which could include CSPs) to "provide assistance in giving effect to the [equipment interference] warrant." Clause 101 explicitly applies this duty to "relevant telecommunications providers." Under these two clauses, communications service providers could be compelled to take any steps, unless "not reasonably practicable", to assist the police and the intelligence services to hack our computers and other devices.

21. While we do not know what this assistance might look like in practice, it could include compelling communication service providers to send false security updates to a consumer in

---

9 President's Review Group on Intelligence and Communications Technologies (12 December 2013) Liberty And Security in a Changing World [Online]. Available from: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [Accessed 26 November 2015]

10 Clause 83, Part 5- Equipment Interference, Draft Investigatory Powers Bill

11 Section 2.12, Equipment Interference: Draft Code of Practice, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473664/EQUIPMENT_INTERFERENCE_CoP.PDF

order to install malware that the police or intelligence services could then use to control the consumer's computer. Security updates are fundamental to protecting all of our devices from unauthorised intrusion, including from cyber criminals and foreign governments. Governments around the world encourage the downloading and installation of software updates as a critical cyber security measure. One UK Home Office cyber security education campaign explains, "Software updates contain vital security upgrades which help protect your device from viruses and hackers [..,] While it's easy to hit 'cancel' and go back to what you're doing, the few minutes it takes to download and install the software updates could save you an enormous amount of time and trouble in the long run."[12] If the draft IP Bill's hacking assistance power is used to co-opt security updates, it would undermine trust in them, which in turn might lead consumers not to install them, leaving them open to crime and a myriad of privacy intrusions.

22. Conceivably, the communication service providers could also be requested to host a "watering hole" attack, by installing custom code on a website they operate that will infect with malware any device that visits that website. For example, the US Federal Bureau of Investigation (FBI) has admitted to deploying such an attack on the servers of the service Freedom Hosting. Each server was turned into a watering hole, and subsequently infected with malware any device that visited the server whether or not that device was of interest to the FBI.[13] It is worth noting that the general public is likely never to be made aware of what kind of "hacking" assistance has been required by communication service providers due to the very strict non-disclosure provision in the Bill (Clause 102.) The negative effect that the secrecy about the employment of these intrusive surveillance techniques could have on the trust of individuals to use internet and other modern form of telecommunications is likely to be huge although difficult to estimate.

Removal of Electronic Protections

23. Beyond the specific provisions regulating hacking capabilities, the draft IP Bill includes, in Part 9, entitled "Miscellaneous and general provisions", additional powers entrusted to the Secretary of State. These powers would allow the UK government to oblige communication service providers to do what it is considered "reasonable" to implement and assist in the implementation of the various surveillance capabilities envisaged in the IP Bill.

24. The list of such "obligations" is broad and open-ended. Notably, the Clause 189 (4c) of the IP Bill would impose "obligations relating to the removal of electronic protection applied by a relevant operator to any telecommunications or data". These obligations are on top of those placed on telecommunications services to assist in "giving effect" to interception warrants (Clause 31) and other similar clauses elsewhere in the Bill (see Clauses 101, 116(5) and 130(5)). Together, these are an indirect attack on end-to-end encryption, which the Government has previously stated it would not undermine. These measures would weaken internet security as they may be interpreted as requiring communication service providers to create "backdoors" to encrypted systems, leaving them open to breaches. This weakened security would also potentially undermine confidence in the British industry. The infrastructure of the internet relies on high encryption standards and this new legislation should do nothing to undermine this.

---

12 HM Government, Installing software updates [Online]. Available from: https://www.cyberstreetwise.com/software-updates [Accessed 26 November 2015]

13 Poulsen, K. (13 September 2013) FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, *Wired* [Online]. Available from: http://www.wired.com/2013/09/freedom-hosting-fbi/ [Accessed 1 October 2015]

25. Encryption underpins the secure functionality of the internet and facilitates global online commerce. The digital economy would be impossible without the use of encryption as it ensures that online transactions remain secure and our personal data is not captured and exploited. As noted by a group of leading technology experts, “It is impossible to operate the commercial Internet or other widely deployed global communications network with even modest security without the use of encryption.”[14]

Data Retention

26. Part 4 of the IP Bill empowers the Secretary of State to require communications service providers to retain communications data (and entity data) for up to 12 months. This requirement is mandatory for providers located in the UK, and requested of those outside the UK.[15] Communications service providers may be required to retain not only data they save in their normal course of business, but also anything they may be able to generate or obtain, including Internet Connection Records.[16]

27. The retained data will potentially include the who, what, where, when, and how relating to every communication that a person has online. This includes, but is not limited to, visited websites, email contacts, to whom, where, and when an email is sent, map searches, GPS location, and information about every device connected to every wifi network in the United Kingdom, which includes Smart Tech such as Nest, iKettle, Smart Barbie, Amazon Echo, and others. The sheer volume of retained data will be huge.

28. Requiring communications service providers to retain all of our revealing and personal data for twelve months treats us all as suspects, undermining the trust we place in government to only exercise its power to intrude upon on personal lives in the most limited and necessary of circumstances.

29. Due to the revealing nature of such data, the database(s) where this retained data is stored are also likely to be targeted by cyber criminals and foreign intelligence agencies. Compelled retention unnecessarily endangers the security communications service providers who could be subject to increased attacks. This year alone has seen the successful infiltration and hacking of several large databases. Recent examples include, but are not limited to, TalkTalk, Vodafone, British Gas, as well as the detrimental Office of Personnel Management (OPM) breach in the United States.[17] Clause 74 of the IP Bill imposes some general obligations to protect the security of such retained data, but its broad provisions are far from a guarantee that future attacks such as these would be prevented. Communications

---

14 Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications [Online]. Available from: https://s3.amazonaws.com/s3.documentcloud.org/documents/2158970/data-security-report.pdf [Accessed 26 November, 2015]

15 Clauses 71 & 79, Part 4, Draft Investigatory Powers Bill

16 Clause 71, Part 4, Draft Investigatory Powers Bill

17 (27 February, 2015) Customer Data Stolen in TalkTalk Hack Attack, BBC Technology [Online] Available from: http://www.bbc.co.uk/news/technology-31656613 [Accessed 26 November, 2015], (31 October, 2015) Vodafone customers' bank details 'accessed in hack', company says, The Guardian [Online] Available from: http://www.theguardian.com/business/2015/oct/31/vodafone-customers-bank-details-accessed-in-hack-company-says [Accessed 26 November, 2015], Hern, Alex (29 October, 2015) British Gas denies responsibility for 2,200 user accounts posted online, The Guardian [Online] Available from: http://www.theguardian.com/technology/2015/oct/29/british-gas-denies-responsibility-user-accounts-posted-online-pastebin [Accessed 26 November, 2015], Hirschfeld Davis, Julie (9 July, 2015) Hacking of Government Computers Exposed 21.5 Million People, The New York Times [Online] Available from: http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html [Accessed 26 November, 2015]

service providers bare the brunt of public criticism in the face of data breaches, even where they are being compelled to retain the data, further undermining trust in the security of their services.

30. As discussed above, the draft IP Bill requires communications service providers to weaken their system security while simultaneously increasing how valuable they are as targets. This potent combination will result in a fundamental weakening the security of communications systems overall in the United Kingdom.

31. Thank you for your consideration of these comments. We are content to have this submission published and attributed to our organisation. If we may be of any additional assistance, we may be contacted as described below.

Privacy International
62 Britton Street
London EC1M 5UY
Tel. 020 3422 4321
info@privacyinternational.org