CENTER FOR DEMOCRACY & TECHNOLOGY

Written evidence submitted by the Center for Democracy & Technology to the Public Bill Committee regarding the Investigatory Powers Bill

23 March 2016

I. Introduction

1. The Center for Democracy and Technology is a non-governmental organisation that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communications technologies. Since its founding more than 20 years ago, CDT has played a leading role in shaping policies, practices, and norms that empower individuals to use these technologies effectively as speakers, entrepreneurs, and active citizens. The organisation is based in Washington, DC, and actively contributes to efforts around the world to ensure that surveillance practices respect human rights.

2. The rights and freedoms affected by the Investigatory Powers Bill – privacy rights and the freedoms of expression, opinion, and association – are among the most valued human rights.[1] Given the degree to which the Bill threatens to undermine them, we hope the Committee will closely scrutinise the issues raised below.

3. This document highlights some, but not all, of the ways in which this Bill would undermine human rights, and includes suggested amendments. First, bulk powers should be removed, and classes of targets for thematic warrants should be narrowed, because each warrant should be based on individualised suspicion. Second, the Bill should be amended to make clear that it does not authorise the government to compel companies to decrypt end-to-end communications. This would undermine or eliminate an important – and in many countries necessary – privacy safeguard. Third, equipment interference powers should be described with greater specificity and narrowed substantially. The broad descriptions of these powers fail to satisfy legality requirements outlined by the European Court of Human Rights. Fourth, provisions limiting a Judicial Commissioner's scope of review to the judicial review standard should be removed, such that Commissioners are permitted to review substantive findings of a decision in addition to procedural aspects of the decision. This will ensure that an authority at least somewhat independent of the executive branch can confirm that the executive branch is not abusing its powers.

II. The scope of surveillance powers should be narrowed

4. While Committee members have surely heard this repeatedly over the past several months, we cannot stress enough the dangers bulk and thematic warrant powers pose to human rights. These powers are excessively intrusive. They would result in undue interference with the right to privacy and chill the exercise of other fundamental rights. If these provisions remain in the Bill when it is enacted, the law will breach binding European human rights law.

[1] Universal Declaration of Human Rights, Articles 12, 19, and 20, U.N. Doc. A/810 (1948); International Covenant on Civil and Political Rights, Articles 17, 19, 21, and 22, U.N. Doc. A/6316 (1966); European Convention on Human Rights, Articles 8, 10, and 11, available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

a. Bulk powers undermine the spirit of privacy rights

5. Bulk powers undermine the spirit of privacy rights.[2] They make privacy intrusion the norm, and protection from intrusion the exception to the norm, by permitting widespread and indiscriminate surveillance.[3] Bulk interception powers permit the government to access any communication they are capable of accessing in the world, unless the sender or recipient is in the British Islands.[4] A bulk acquisition warrant allows the government to collect any communications data 'relating to the acts or intentions of persons outside the British Islands', which does not seem to preclude access to data solely from people within the British Islands.[5] Bulk equipment interference permits the 'hacking' of many computers and personal devices simultaneously, as discussed below.[6] These powers potentially interfere with almost all telecommunications users' privacy rights.

b. Warrants must be based on individualised suspicion

6. Secret surveillance violates the European Convention on Human Rights if it is not based on individualised suspicion. According to the European Court of Human Rights, an authorisation for interception must 'clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered'.[7]

7. As discussed above, bulk warrants by definition are not based on individualised suspicion.

8. Thematic warrants, while described in chapters related to targeted surveillance, are akin to bulk powers. They permit the surveillance of a 'group of persons who share a common purpose or who carry on, or may carry on, a particular activity' and 'more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purpose of a single investigation or operation . . .'.[8] These definitions could encompass, for example, all members of a particular religion or political party. Bulk warrants therefore would not necessarily be based on individualised suspicion.

c. Warrants should be narrowly targeted

9. We recommend Parliament withhold the power to issue bulk warrants, and narrow the classes of targets for thematic warrants.

10. To ensure that warrants are based on individualised suspicion, the government could borrow from language appearing in the USA FREEDOM Act. Applications for telephonic surveillance must refer to a 'specific selection term', which is an identifier

[2] Joseph A. Cannataci, Report of the Special Rapporteur on the right to privacy [Advanced unedited version], U.N. Doc. A/HRC/31/64, § 39 (8 March 2016), available at: http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc (stating 'bulk interception and bulk hacking . . . undermine the spirit of the very right to privacy'.).
[3] Zeid Ra'ad Al Hussein, The right to privacy in the digital age, U.N. Doc. A/HRC/27/37, pages 8-9 (2014) (stating 'the restrictions [on a right] must not impair the essence of the right . . . . [T]he relation between right and restriction, between norm and exception, should not be reversed'.).
[4] Investigatory Powers Bill, § 119(2-3).
[5] *Ibid*. at § 138(3).
[6] *Ibid*. at § 154(1-2).
[7] Zakharov v. Russia, ECtHR, Judgment (4 Dec. 2015), § 264.
[8] Investigatory Powers Bill, § 15(2)(a-b); see also § 90(1-2).

– e.g., a phone number or email address – that identifies a specific person, account, address, or personal device for surveillance.[9]

III. The Bill should not undermine end-to-end encryption

11. In a submission to the Joint Committee on the Draft Investigatory Powers Bill, we asked that the revised Bill clarify whether 'the government can compel service providers to cease offering end-to-end encryption in their products and services'.[10] The revised Bill fails to answer this question, so we recommend that the Bill explicitly state that a service provider cannot be compelled to stop offering end-to-end encrypted communications or create backdoors.

a. Backdoors compromise security

12. End-to-end encryption 'scrambles' a communication in transit, so that only the sender and recipient, and not the service provider or manufacturer, can read it by decrypting the communication with a special encryption key. A service provider or manufacturer can gain access to end-to-end encrypted communications by developing or maintaining a 'backdoor', which is an exceptional access mechanism that allows parties other than the sender and recipient to decrypt content.

13. Manufacturers, service providers, and technologists object to backdoors because they are easily exploited and very difficult to secure, and therefore make end-to-end encryption ineffective and brittle.[11] Government officials who claim it is possible to maintain backdoors without compromising security tend not to understand the technical aspects of encryption.[12]

14. Human rights experts also oppose the undermining of encryption. It plays an important role in protecting privacy rights and the freedoms of speech, opinion, and association, especially in countries governed by authoritarian regimes.[13] It is also used worldwide by journalists, lawyers, and other professionals whose ethical standards require confidentiality.[14] It would set a bad precedent for the rest of the world, including authoritarian governments, if the UK were to undermine encryption by requiring backdoor access to communications.[15]

---

[9] 50 U.S.C. § 1861(k)(4)(A)(i)(I) (2016), available at: http://uscode.house.gov/view.xhtml?req=(title:50%20section:1861%20edition:prelim)%20OR%20(granuleid:USC-prelim-title50-section1861)&f=treesort&edition=prelim&num=0&jumpTo=true.

[10] CDT, Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill, § 6 (21 Dec. 2015), available at: https://cdt.org/files/2016/01/CDT-UKIPBJointCommittee-1221submission.pdf.

[11] See, e.g., Tim Cook, A Message to Our Customers (16 Feb. 2016), available at: http://www.apple.com/customer-letter/; Cindy Cohn, The Debate Over Encryption: The Backdoor Is a Trap Door, Wall Street Journal (23 Dec. 2015), available at: http://www.wsj.com/articles/the-debate-over-encryption-the-backdoor-is-a-trapdoor-1450914316.

[12] See, e.g., Mark Sullivan, Source: Members of Congress Dismayed by FBI Director's Lack of Tech Knowledge, Fast Company (12 March 2016), available at: http://www.fastcompany.com/3057768/source-members-of-congress-dismayed-by-fbi-directors-lack-of-tech-knowledge.

[13] See, e.g., David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015); UN OHCHR, Apple-FBI case could have serious global ramification for human rights: Zeid (4 March 2016), available at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E/.

[14] See, e.g., Kaye, *supra* at footnote 13, §§ 1, 48, and 59.

[15] UN OHCHR, *supra* at footnote 13 (stating that mandated encryption backdoors are 'potentially a gift to authoritarian regimes, as well as to criminal hackers'.).

b. The government have been unclear about whether the Bill requires backdoors

15. In our submission to the Draft Bill Joint Committee, we noted that 'Under current legislation, UK authorities have the power to order users or communications service providers to decrypt communications, at least where the individual or company concerned has the encryption keys (or otherwise has the ability to decrypt the information). However, for CSPs that have secured their customers' communications using end-to-end encryption, it has been considered a reasonable response to a RIPA § 49 notice for a CSP to say that it cannot turn over encryption keys it does not possess'.[16]

16. Although § 217(4)(c) of the revised Bill seems to suggest that obligations in the technical capability notices relate only to 'electronic protection applied by or on behalf of that operator to any communications or data', the government have not yet clarified whether it will remain a reasonable response for a CSP to say that it cannot turn over encryption keys it does not possess (or the underlying data that have been encrypted with keys it does not possess).

17. It is therefore crucial that the Committee press the Secretary of State to clarify whether, under § 217(3)(a-b), she considers it 'practicable to impose requirements' in circumstances where end-to-end encryption is being applied by an operator, and if those requirements would prevent a CSP from providing end-to-end encryption.

18. If the Secretary *does* consider it practicable, then we foresee two scenarios:

    i) Either it will no longer be possible to offer end-to-end encryption in the UK; or

    ii) Companies can continue to offer end-to-end encryption, but will be forced, likely under an interference warrant, to write software that *secretly* removes it from certain users' devices without users' knowledge.

19. We therefore recommend an amendment to the Bill that plainly states it would not be considered reasonable and practicable to require the decryption of end-to-end encrypted communications.

IV. Equipment interference capabilities should be described in greater detail

20. Equipment interference is both less understood by the public and more intrusive than other surveillance methods. The Bill fails to properly inform the public by specifying which methods of equipment interference are permissible, rendering the Bill inadequate under European human rights law. Therefore, the Bill's equipment interference provisions should be rewritten in a more detailed way.

a. Equipment interference is very intrusive

21. Equipment interference – or 'hacking' – allows one to access and manipulate another's computer or personal device. A summary of equipment interference methods appears in evidence submitted by Privacy International and Open Rights Group:

> 'The intelligence agent can access any stored data, including documents, emails, diaries, contacts, photographs, internet messaging chat logs, and

[16] See, e.g., CDT, *supra* at footnote 10, § 45.

location records on mobile equipment. He can see anything typed into the device, including login details and passwords, internet browsing histories and draft documents and communications the user never intended to share. He can recover files that have been deleted. He can control any functionality, including surreptitiously turning on the microphone, webcam and GPS-based locator technology. He can even re-write the code that controls the device, adding new capabilities and erasing any trace of his intrusion'.[17]

b. The government should satisfy their obligation to provide adequate detail

22. The Bill describes the government's equipment interference powers only generally. Targeted equipment interference and examination warrants permit 'any conduct . . . necessary' to obtain communications, equipment data, or 'any other information'.[18] This conduct includes, but is not limited to, 'monitoring, observing or listening to a person's communications or other activities', and 'recording anything which is monitored, observed or listened to'.[19] As with other investigatory powers, a targeted warrant can be issued on the grounds of national security, the prevention or detection of serious crimes, and the economic wellbeing of the UK when national security is involved, when it is necessary and proportionate.[20] The Equipment Interference Draft Code of Practice elaborates on these topics, but only partially.[21]

23. The European Court of Human Rights requires secret surveillance to be conducted in accordance with the law.[22] In part, this means that a law must be detailed and 'sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which' government surveillance can be based.[23] Clarity and detail help to prevent the arbitrary use of powers.[24]

24. Because this Bill is so unspecific about equipment interference capabilities, the Court would most likely find that it fails to satisfy this legality requirement.

25. Equipment interference provisions in the Bill or the draft code of practice should list which types of equipment interference are permissible.

V. A Judicial Commissioner's scope of review should not be limited to the judicial review standard

26. The language of the Bill should be changed to ensure that a Judicial Commissioner will independently assess the merits of each warrant. If Commissioners are limited to reviewing mainly procedural aspects of the decision-making process under the

[17] Privacy International and Open Rights Group, Submission in Response to the Consultation on the Draft Equipment Interference Code of Practice, page 4 (20 March 2015), available at: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf.
[18] Investigatory Powers Bill, § 88(2-5) and (9).
[19] *Ibid*. at § 88(4)(a-b).
[20] *Ibid*. at § 91(5).
[21] For example, the draft Code helpfully states that an interference is disproportionate 'if the material which is sought could reasonably be obtained by other less intrusive means'. Home Office, Equipment Interference Draft Code of Practice, § 3.26 (Spring 2016), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504238/Equipment_interference_draft_code_of_practice.PDF. It also provides a few examples of methods of equipment interference. *Ibid*. at § 2.4.
[22] See, e.g., Szabó and Vissy v. Hungary, European Court of Human Rights [ECtHR], Judgment (12 Jan. 2016), §§ 58-62.
[23] *Ibid*. at § 62.
[24] *Ibid*. at § 65.

judicial review standard, they will be unable to prevent the abuse of the executive branch's great discretion in surveillance matters.

a. A judge must independently assess the merits of each warrant

27. Both international norms and binding European human rights law demand that a judge independently review all relevant facts before making a decision.

28. Judicial codes of ethics worldwide, as distilled into the UN's Bangalore Principles, require that a judicial assessment be made 'independently on the basis of the judge's assessment of the facts . . . free of any extraneous influences . . . from any quarter for any reason'.[25]

29. The European Court of Human Rights specifically demands merit-based judicial authorisation, or something functionally equivalent, for surveillance applications. The Court has found a violation of privacy rights under the Convention where a law allowed approval of surveillance warrants without ensuring that the authorising authority independently assessed the merit of each application.[26] 'For the Court, only [information about the factual basis of suspicion] would allow the authorising authority to perform an appropriate proportionality test'.[27] Review by an authority other than a judge is permissible as long as he or she is sufficiently independent from the executive.[28]

b. Judicial review would not require a review of the merits of a warrant

30. The Bill requires a Judicial Commissioner to approve most warrants issued by the Secretary of State or other appropriate authority, but limits the grounds on which a Commissioner may reject a warrant. The Bill states that a 'Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review'.[29]

31. According to the official website of the Judiciary, judicial review is a 'challenge to the way in which a decision has been made, rather than the rights and wrongs of the conclusion reached'.[30] 'It is not really concerned with the conclusions of that process and whether those were "right", as long as the right procedures have been followed. The court will not substitute what it thinks is the "correct" decision'.[31] This understanding of judicial review has been echoed by almost every legal expert who has provided evidence on the topic.[32]

---

[25] Judicial Group on Strengthening Judicial Integrity, The Bangalore Principles of Judicial Conduct (2002), § 1.1, available at: http://www.unodc.org/pdf/crime/corruption/judicial_group/Bangalore_principles.pdf.
[26] See, e.g., Szabó and Vissy v. Hungary, *supra* at footnote 22, §§ 71 and 88 (finding a violation of Article 8, in part, because applications for surveillance were not supported with a sufficient factual basis or supporting materials); Zakharov v. Russia, ECtHR, Judgment (4 Dec. 2015), §§ 262-63 and 305 (finding a violation of Article 8, in part, because judges regularly approved requests for secret surveillance without verifying the existence of reasonable suspicion against each target, often because supporting materials were not received or requested).
[27] Szabó and Vissy v. Hungary, *supra* at footnote 22, § 71.
[28] See, e.g., Weber and Saravia v. Germany, ECtHR, Decision (29 June 2006), §§ 24-25 and 138 (describing acceptable oversight bodies composed of members of parliament and people qualified to hold judicial office).
[29] Investigatory Powers Bill § 21(2); see also §§ 97(2), 123(2), 139(2), 157(2), and 179(2).
[30] Courts and Tribunals Judiciary, Judicial review, para. 2, available at: https://www.judiciary.gov.uk/you-and-the-judiciary/judicial-review/.
[31] *Ibid*. at para. 3.
[32] See, e.g., Privacy International, Liberty, and Big Brother Watch, Oral Evidence Taken Before the Joint Committee, Q 129 (9 Dec. 2015), available at: http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf.

32. When questioned about the judicial review standard, the Secretary of State was unclear about how it would be applied. She seemed to hint that a Judicial Commissioner would be able to review the merits of each warrant: 'There may well be circumstances in which they might apply a lighter-touch approach to reviewing a Secretary of State's decision, and others in which they will look more at necessity and proportionality'.[33] Yet she also stated that Judicial Commissioners 'are not re-taking the decision'.[34] Given the Secretary's evasiveness, and given the fact that these provisions remain in the Bill despite prior evidence raising the issue, it appears that the government do intend to limit the scope of review.

33. The provisions referencing judicial review should be removed from the Bill. The logical reading of the Bill absent these provisions would call for a review of the facts by the Judicial Commissioner, ensuring an independent assessment.

VI. Conclusion

34. Although this evidence focuses only on the Bill's flaws, it is important to note that the Bill presents an opportunity for the government to set a good example for the rest of the world.[35] The government have already made great progress simply by publicising all of their secret surveillance powers in a statute to which they can be held accountable. They should now take full advantage of this opportunity by addressing the issues outlined above.

[33] Theresa May MP, Oral Evidence Taken Before the Joint Committee, Q273 (13 Jan. 2016), available at: http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf.
[34] *Ibid*.
[35] See Cannataci, *supra* at footnote 2, § 39 ('Bearing in mind the huge influence that UK legislation still has in over 25% of the UN's members states that still form part of the Commonwealth, as well as its proud tradition as a democracy which was one of the founders of leading regional human rights bodies such as the Council of Europe, the SRP encourages the UK Government to take this golden opportunity to set a good example and step back from taking disproportionate measures which may have negative ramifications far beyond the shores of the United Kingdom'.).