KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY
& TECHNOLOGY

Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill

Center for Democracy & Technology (21 December 2015)

I. Introduction

1. The Center for Democracy & Technology ('CDT') welcomes this opportunity to submit written evidence to the Parliament of the United Kingdom's Joint Committee ('the Committee') on the Draft Investigatory Powers Bill ('Draft Bill'). CDT is a non-profit organization that works to preserve the user-controlled nature of the Internet and champion freedom of expression around the world.

II. Summary

2. Many of the powers in the Draft Bill are plainly incompatible with the ECHR or EU law. (¶¶ 7–18)
    a. The surveillance authorisation scheme set out in the Draft Bill is incomplete and falls short of human rights standards. (¶¶ 9–11)
    b. Legislation providing for data retention notices that could potentially require the retention of the communications data of every individual in the UK is manifestly incompatible with the rights to privacy and the protection of personal data. (¶¶ 12–14)
    c. Provisions for 'targeted' surveillance or equipment interference do not create the level of foreseeability required by the ECHR or impose legal protections sufficient to ensure that all interferences with privacy rights are strictly necessary, proportionate and non-discriminatory. (¶¶ 15–18)
    d. We make recommendations with respect to human rights law in ¶ 24.
3. The definitions in the Draft Bill are insufficiently narrowly defined. (¶¶ 25–30)
    a. We recommend that (1) definitions should be narrow, technically-grounded, and unambiguous so as to make clear the intended scope of powers and (2) updates to definitions in the statute should be: (a) approved by a vote of the Technical Advisory Board contemplated in the Draft Bill and (b) provided for by means of an affirmative Statutory Instrument, to ensure Parliamentary oversight.
4. The level of intrusiveness of IP resolution into private lives of innocent people is disproportionate, and, we believe, contravenes the ECHR and the Charter of Fundamental Rights of the European Union. (¶¶ 31–37)

1634 I Street, NW
Suite 1100
Washington, DC 20006

a. CDT recommends that the requirement to create and retain ICRs be struck from the bill entirely, and that targeted data preservation orders be used instead.

5. Both targeted and bulk equipment interference pose grave risks and should be narrowed substantially. (¶¶ 38–43)
    a. The standard for issuing an EI warrant should require that EI should only be used where other means are not available/feasible.
    b. Neither the police nor the security and intelligence services should have access to powers to undertake bulk equipment interference.
    c. The government should clarify what conduct can and cannot be authorised in an interference warrant.
6. The Draft Bill should clarify whether the government can compel service providers to cease offering end-to-end encryption in their products and services. (¶¶ 44–48)

III. Are the powers compatible with the Human Rights Act and the European Convention on Human Rights ('ECHR')?

7. Many of the powers in the Draft Bill are plainly incompatible with the ECHR or EU law.

8. We recall at the outset that under Article 8 of the ECHR, *'powers of secret surveillance of citizens, characterising as they do the police state, are tolerable … only in so far as strictly necessary for safeguarding the democratic institutions.'*[1] It is our view that the exercise of surveillance powers is permissible under the Convention only where this heightened standard is met, and not merely where the collection or retention of data – or surreptitious interference with devices – would be, or could someday prove to be, convenient for the authorities. We observe that

[1] *Klass and others v Germany*, [1978] ECHR 4, Judgment (Plenary), 6 Sept. 1978, ¶ 42; see also *Rotaru v Romania*, [2000] ECHR 192, Judgment (Grand Chamber), 4 May 2000, ¶ 47; *Kennedy v the United Kingdom*, [2010] ECHR 682, Judgment, 18 May 2010, ¶ 153.

the Court of Justice of the EU ('CJEU') has adopted similar language in cases concerning data retention and surveillance.[2]

A. The surveillance authorisation scheme

9. **As an initial matter, the surveillance authorisation scheme set out in the Draft Bill is incomplete and falls short of human rights standards, notwithstanding the fact that it may represent some degree of improvement over the current system.** As we have pointed out in written evidence submitted to the Joint Committee on Human Rights,[3] Article 8 of the ECHR requires that all secret surveillance practices must be *'subject to effective supervision'* by the judiciary or, at minimum, a similar body that is *'independent of the authorities carrying out the surveillance'*.[4] Under the proposed scheme, however, some highly intrusive surveillance powers, such as the targeted acquisition of communications data, the issuance of data retention notices and the issuance of potentially sweeping national security notices, would not require any form of judicial or equivalent *ex ante* independent approval at all.[5]

10. Moreover, even where the exercise of surveillance powers requires the approval of a judicial commissioner, the commissioner will apply only the attenuated 'judicial review' standard.[6] We believe this form of review cannot be regarded as *'effective supervision'* for the purposes of the Convention.[7]

11. Finally, as detailed in our submission to the Joint Committee on Human Rights, we believe the appointment process and potentially indefinite renewable terms would prevent the judicial commissioners from being fully independent of the Executive – the part of government that will be responsible for conducting much of the

---

[2] *Digital Rights Ireland v Minister for Communications, Marine and National Resources et al*, Judgment, [2014] EUECJ C-293/12, 8 Apr. 2014, ¶ 52; *Schrems v Data Protection Commissioner*, Judgment, [2015] EUECJ C-362/14, 6 Oct. 2015, ¶¶ 92-93.

[3] Center for Democracy & Technology, 'Written evidence submitted by the Center for Democracy & Technology to the Joint Committee on Human Rights regarding the Draft Investigatory Powers Bill', 7 Dec. 2015, https://cdt.org/files/2015/12/CDT-JCHR-written-evidence.pdf.

[4] *Rotaru*, *supra* n. 1, ¶ 59; *Klass*, *supra* n. 1, ¶ 56.

[5] Draft Investigatory Powers Bill (hereinafter 'Draft Bill'), §§ 46, 71 and 188.

[6] See, e.g., *ibid.* at § 19(2).

[7] *Rotaru*, *supra* n. 1, ¶ 59.

surveillance – in violation of the ECHR's independence requirements.[8] Where the renewable nature of the commissioners' terms is concerned, we observe that by contrast, judges appointed to the Foreign Intelligence Surveillance Court in the United States serve single, non-renewable terms of no more than seven years (whilst otherwise continuing to enjoy the life tenure guaranteed to federal judges under Article III of the US Constitution).[9]

B. Data retention and bulk powers

12. **In our view, legislation providing for data retention notices that could potentially require the retention of the communications data of every individual in the UK is manifestly incompatible with the rights to privacy and the protection of personal data, as found in the Charter of Fundamental Rights of the European Union ('the Charter') and applied by the CJEU in its *Digital Rights Ireland* judgment.[10]** In that case, the Court invalidated the Data Retention Directive not only due to its failure to place firm strictures on access to the data, but, first and foremost, because it:

    a. *'cover[ed], in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime'*;[11]

    b. did not include exceptions for *'persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy'*;[12] and

---

[8] See *Rotaru*, *supra* n. 1, ¶ 59; *Klass*, *supra* n. 1, ¶ 56.

[9] 50 U.S.C. § 1803(d).

[10] Charter of Fundamental Rights of the European Union, Articles 7 and 8; *Digital Rights Ireland, supra* n. 2, ¶¶ 45-69.

[11] *Digital Rights Ireland*, supra n. 2, ¶ 57; see also *Schrems*, supra n. 2, ¶ 93 (*'Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to'* a third country *'without any differentiation, limitation or exception being made in the light of the objective pursued'*). Much of the language in this section of our submission is drawn from *Center for Democracy & Technology and Privacy International, Third-party intervention*, Conseil d'État (France), Contentious Section, N° 393099: FDN et al. c/ Gouvernement (forthcoming).

[12] *Digital Rights Ireland*, supra n. 2, ¶ 58.

c. did not *'require any relationship between the data whose retention [was] provided for and a threat to public security'*: in particular, it failed to require a link, *'even an indirect or remote one'*, between the persons affected and serious crime, and further failed to place temporal or geographic limitations on the data to be retained.[13]

13. The data retention notices contemplated in the Draft Bill clearly violate EU law as these three elements from the *Digital Rights Ireland* judgment directly apply. There is also a strong likelihood that they violate Article 8 of the ECHR, which the European Court of Human Rights ('ECtHR') has previously interpreted as prohibiting a scheme under which the UK authorities, in a *'blanket and indiscriminate'* fashion, had the power to retain the biometric information of individuals who had not been convicted of a crime.[14]

14. For the same reasons, we believe the bulk powers contemplated by the bill are incompatible with EU law[15] and the ECHR at least insofar as they could be read to permit the indiscriminate and indefinite surveillance of (or equipment interference affecting) individuals for whom there is no suspicion of wrongdoing. Such powers, both separately and – especially – in the aggregate, are plainly incompatible with the very notion of a democratic society.

C. 'Targeted' surveillance that may be discriminatory or excessive

15. Even where the surveillance or equipment interference contemplated by the Draft Bill is ostensibly 'targeted', we are gravely concerned that the relevant provisions do not create the level of foreseeability required by the ECHR or

---

[13] *Ibid.* at ¶¶ 58-59; cf. *Schrems*, *supra* n. 2, ¶ 93 (indicating that legislation concerning the storage of personal data must set out *'an objective criterion … by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference'* which access to and use of the data entail).

[14] *S and Marper v the United Kingdom*, Nos 30562/04 & 30566/04, Judgment (Grand Chamber), 4 December 2008.

[15] See Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Articles 5(1) and 15(1) (requiring Member States to prohibit surveillance and storage of communications or traffic data, and mandating that any exceptions to this requirement based on national security, the prevention and prosecution of criminal offences, etc., must 'constitute[] a necessary, appropriate and proportionate measure within a democratic society').

impose legal protections sufficient to ensure that all interferences with privacy rights are strictly necessary, proportionate and non-discriminatory.

16. In particular, we note that under the Draft Bill, 'targeted' interception and equipment interference warrants could relate to *'a group of persons who share a common purpose or who carry on, or may carry on, a particular activity'*.[16] We recall the ECtHR's repeated statement that any domestic law authorising secret surveillance measures *'must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures'*.[17] In our view, the Draft Bill's reference to *'a group of persons who ... carry on, or may carry on, a particular activity'* is so facially vague as to breach this aspect of the legality requirement of Article 8 of the Convention. Such language does not, by its terms, exclude the possibility that everyone who belongs to a certain trade union, political party or book club; visits a certain shop; attends (or has friends or family members who attend) a certain house of worship; subscribes to a certain publication; participates in a lawful and peaceful demonstration; celebrates or may celebrate a certain religious or national holiday; or uses a particular e-mail or instant messaging service may experience very serious privacy intrusions pursuant to a 'targeted' warrant in a manner that cannot reasonably be regarded as foreseeable. It also does not provide adequate protection against the possibility that 'group[s]' will be targeted for privacy interferences in a manner that violates the anti-discrimination provision of the ECHR (Article 14).

17. Furthermore, multiple provisions of the Draft Bill would allow the government, after obtaining a judicial commissioner's approval of a surveillance warrant, to engage in *'**any conduct** which it is necessary to undertake in order to do what is expressly authorised or required'* by the warrant – including, for example, *'the interception of communications not described in the warrant'* (emphasis added).[18] Such provisions give rise to a serious risk that any necessity and proportionality analysis undertaken by the authority issuing the warrant, as well as any review undertaken by the judicial commissioners, will be largely illusory, and that in practice the relevant surveillance

---

[16] Draft Bill, *supra* n. 5, §§ 13(2) and 83.

[17] See, e.g., *Weber and Saravia v Germany*, No 54934/00, Decision, 29 June 2006, ¶ 93; *Liberty and ors v the United Kingdom*, No 58243/00, Judgment, 1 July 2008, ¶ 62; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, No 62540/00, Judgment, 28 June 2007, ¶ 75.

[18] Draft Bill, *supra* n. 5, §§ 12(5), 81(5), 106(5), 122(7) and 135(4).

activity will far exceed what is *'strictly necessary for safeguarding the democratic institutions'* (see above).

18. Our concerns about the Draft Bill's incompatibility with the ECHR and EU law extend beyond these aspects of the text, and we would welcome opportunities to submit additional remarks.

D. Additional evidentiary questions

19. We provide some additional responses to questions the Committee has asked here.

1. Is the authorisation process appropriate?

20. No. Please see paragraphs 9–11, and 17 above, as well as our written evidence submitted to the Joint Committee on Human Rights.[19]

2. Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland judgment?

21. No; see paragraphs 12–13 above.

3. Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

22. No. Please see paragraphs 9–11, and 17 above, as well as our written evidence submitted to the Joint Committee on Human Rights.[20]

[19] *Supra* n. 3.

[20] *Ibid.*

4. Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

23. No. Please see paragraphs 9–11 above, as well as our written evidence submitted to the Joint Committee on Human Rights.[21]

E. Human Rights Recommendations

24. The Committee has asked *'Are the powers compatible with the Human Rights Act and the European Convention on Human Rights ('ECHR')?'*, and our answer is clearly no. The Committee should recommend that the Draft Bill be amended to:

    a. Provide that judicial commissioners must be nominated and confirmed by entities that are independent of the Executive and contain strong indicia of democratic legitimacy.

    b. Empower judicial commissioners to review all of the factual circumstances and legal evaluations underlying a warrant or other exercise of surveillance powers before deciding whether to approve it.

    c. Extend the review and authorisation powers of the judicial commissioners to all forms of privacy interferences contemplated by the Draft Bill.

    d. Provide that the terms served by judicial commissioners are strictly limited to a predetermined period of years and are not renewable.

    e. Narrow all of the surveillance powers in the Draft Bill (including data retention and equipment interference) so as to prohibit effectively the indiscriminate and indefinite surveillance of individuals for whom there is no suspicion of wrongdoing.

    f. Clarify the nature and scope of, and require judicial authorisation for, the national security notices contemplated by § 188 of the Draft Bill so as to mitigate the potential for abuse (e.g. the possibility that such notices will be used to evade judicial authorisation that would otherwise be required).

    g. Restrict the 'targeted' surveillance powers in the Draft Bill in a manner that prevents their use for interferences that are discriminatory or

[21] *Ibid.*

excessive, and ensures that the nature and extent of the surveillance that may occur pursuant to these provisions are fully foreseeable to both the judicial commissioners and the public.

h. Generally, ensure that all interferences with privacy rights through secret surveillance measures meet the heightened standard of being strictly necessary for safeguarding democratic institutions.

IV. Are the powers sought workable and carefully defined?

25. The Committee asks: *'Are the technological definitions accurate and meaningful? Does the Draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall, is the Bill future-proofed as it stands?'*

26. The definitions in the Draft Bill are insufficiently narrowly defined. Definitions should be drafted to map unambiguously onto current features of Internet architecture and protocols so that communications service providers (CSPs) can understand what they will need to collect, retain and be prepared to produce with the proper legal authorisation.

27. We recognise the importance of ensuring that technological developments do not render the powers detailed in the bill ineffective. However, in our view the terminology is currently so broad that there is not only difficulty in mapping the legislative language to actual features of existing technology, but also real uncertainty created with respect to the scope of the powers sought in the Bill.

28. We would particularly like to draw the Committee's attention to the definitions of: 'equipment', 'communications data', 'Internet connection record', 'electronic protection', and 'system' (see paragraph 43, below).[22] Each of these terms – with the exception of 'Internet connection record' – have commonly-accepted technical definitions that should be used instead of the current definitions in the Draft Bill, which are so vague and expansive to hardly be definitional at all.

29. To ensure that the legislation provides for both statutory and technical clarity in addition to 'future-proofing', we recommend that (1) definitions should be narrow, technically-grounded, and unambiguous so as to make clear the intended scope of

[22] § 81(2) and 82(3) & (4).

powers and (2) updates to definitions in the statute should be: (a) approved by a vote of the Technical Advisory Board contemplated in the Draft Bill and (b) provided for by means of an affirmative Statutory Instrument, to ensure Parliamentary oversight.

30. For example, the definition of the elements of an Internet connection record in the Draft Bill match only to some extent standard technical network connection logging facilities such as Netflow (a proprietary Cisco standard) and IPFIX (the non-proprietary equivalent standardized by the Internet Engineering Task Force). However, these technical connection logging standards can only collect lists of IP addresses, not web pages, for which additional information from users' Domain Name System queries must be included – which amounts to incredibly intrusive information, compromising a complete record of what people read and do online.

V. Data Retention

31. The Committee asks, *'Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?'*

32. The level of intrusiveness of IP resolution into private lives of innocent people is disproportionate, and, we believe, contravenes the ECHR and the Charter of Fundamental Rights of the European Union.

33. CDT submitted comments[23] to this effect to the House of Commons Home Affairs Committee's inquiry into the Counter-Terrorism and Security Bill last year. We would like to draw this Committee's attention to that submission and re-emphasise those concerns here.

34. The government have argued in the guidance notes that the bulk retention of Internet Connection Records is necessary to *'identify the communications service to which a device has connected'*, and that this new power is intended to *'restore capabilities that have been lost as a result of changes in the way people*

[23] Center for Democracy & Technology, 'Comments on Part 3 of the draft Counter-Terrorism and Security Bill', submission to the Parliament of the United Kingdom Home Affairs Committee (15 December 2014), *available at:* https://cdt.org/files/2014/12/CDT-UK-CTS-Bill-comments-Part-3.pdf.

communicate'.[24] Evidence from countries where the retention of ICRs has been extensively tried – such as Denmark[25] – suggests they will not be effective for these purposes.

35. We would like direct the Committee's attention to the recent repeal of similar powers by Denmark and to the submission by Danish NGO IT-Pol to the Science and Technology Committee inquiry, which provides detailed evidence regarding the lack of efficacy of ICRs.[26]

36. Additionally, it is important to note that unlike with telephony, the line between communications content and communications data on the Internet is not clear. It is therefore inappropriate, and potentially misleading, to regard ICRs as merely being equivalent to telephone communications data, when in fact they can be even more revealing of private life, for example, effectively serving as a list of materials recently read, viewed, purchased, or otherwise interacted with online.

37. **Given the level of intrusiveness, cost, and ineffectiveness of ICR data retention, CDT recommends that the requirement to create and retain ICRs be struck from the bill entirely, and that targeted data preservation orders (as described in our December 2014 comments[27]) be used instead.**

VI. Equipment Interference

38. The Committee asks, *'Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers? Are the safeguards for such activities sufficient?'*

39. **Neither the police nor the security and intelligence services should have access to powers to undertake bulk equipment interference.** Such a power, for

---

[24] Draft Bill Guidance notes, page 5.

[25] IT-Political Association of Denmark, 'Written evidence submitted by IT-Political Association of Denmark', submission to the Parliament of the United Kingdom Science and Technology Committee (8 December 2015), *available at:* http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25190.html.

[26] *Ibid.*

[27] CDT Counter-Terrorism and Security Bill Comments, *supra,* n. 23.

reasons described earlier in this submission (see paragraphs 15–18), is incompatible with EU law and the ECHR due to its disproportionate nature.

40. CDT is alarmed that the government seeks powers that would require service providers to assist in 'hacking' their own customers. The inclusion of the duty in § 101 to assist in giving effect to interference warrants would undermine UK consumers' trust in UK CSPs and damage UK CSPs' reputations internationally.

41. In addition, we are concerned that:

    a. A 'targeted' interference warrant does not actually target an individual and that a single 'targeted' warrant could end up monitoring many people. For example, §§ 83(d) & (e) allow for interference with any equipment in one or more locations without placing any restrictions on the scope of what is meant by location. Restricting it to 'premises' would narrow the notion of location here to a physical facility, but some facilities (such as data centres and Internet exchange points (IXPs)) contain thousands of pieces of equipment mediating communications between tens to hundreds of thousands of individual people.

    b. Equipment interference, as it necessarily entails 'breaking into' devices and services, could create vulnerabilities in CSPs' systems that could leave them open to hacking and exploitation by criminals, hostile governments or others. These vulnerabilities could damage the ability of CSPs to store the retained data securely as mandated in § 74 of the bill. Any equipment interference must be undertaken with appropriate safeguards that are designed to minimize the impact of impairing equipment and services.

    c. Targeted EI represents an extreme and dangerous form of intrusion. It is paramount that it should only be used in a manner that is strictly lawful, necessary and proportionate (see above) and where other means are not feasible. We note that the Secretary of State, in deciding whether it is 'necessary' to issue an EI warrant, must consider *'whether what is sought to be achieved by the warrant could reasonably be achieved by other means,'* but the standard should instead require that EI should only be used where other means are not available/feasible. (§ 84(6))

42. The government should clarify what conduct can and cannot be authorised in an interference warrant. § 101(1) requires that a CSP that has been served with a warrant *'must take all steps for giving effect to the warrant that are notified to the*

relevant telecommunications provider'. Similarly, although § 40(3) requires bulk equipment interference warrants *'describe the conduct that is authorised by the warrant'* it does not place any restrictions on the conduct that may be authorised. In particular, it may be possible for a bulk EI warrant to include a requirement for a company to assist with the creation of a 'backdoor' into their own encryption technology, an exceedingly dangerous prospect that can threaten the security of all communications mediated by that technology. We would prefer the Draft Bill clearly articulate what classes of interference are possible with an EI warrant, rather than merely providing for notice and a description of the content as a condition of the warrant to issue.

43. The definition of a 'system' should also be more clearly defined. § 81(2) and 82(3) & (4) note that a system is a relevant system if any communications or private information are held on or by means of the system. In the Australian context, similarly overbroad language has been interpreted as potentially including the entire Internet.[28]

VII. Encryption

44. The Draft Bill should clarify whether the government can compel service providers to cease offering end-to-end encryption in their products and services.

45. Under current legislation,[29] 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. In these circumstances, companies would hand over the encrypted communication. The protections encryption provides are critical for private conversations to be possible in online environments. They are particularly important for privileged communications (e.g., Attorney-Client privilege)

[28] Center for Democracy & Technology, Australian Privacy Foundation, New South Wales Council for Civil Liberties, and Privacy International, 'Joint Submission to the United Nations Human Rights Council Twenty-third Session of the Universal Periodic Review Working Group' (November 2015), *available at:* https://cdt.org/insight/expert-report-led-by-cdt-finds-that-australian-surveillance-violates-human-rights/.

[29] RIPA, § 49 http://www.legislation.gov.uk/ukpga/2000/23/section/49

and sensitive finance, health, business, and critical infrastructure (power, water, public health, &c) communications.

46. The Draft Bill replaces the current obligation to maintain permanent interception capability[30] with one that requires CSPs to maintain permanent capabilities *'relating to the powers specified under the Draft Bill.'* Those capabilities, which are set out in § 189, include *'obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data'*. This obligation is of particular concern.

47. The government have stated that the new legislation *'will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA.'.*[31] However, although the Draft Bill does not ban encryption, in practice it will be possible under the new bill for the Home Secretary to issue a § 198 'Technical Capability Notice' imposing obligations on CSPs which could prevent them from protecting communications through end-to-end encryption.

48. The ambiguity created by the provisions in the bill relating to encryption raises a critical question: is it the governments' intention to be able to mandate backdoors in communications by issuing notices – both domestically and to companies overseas – that would prevent the application of end-to-end encryption? Such a move would lead to a loss of confidence in UK technology companies globally and would damage investment in the broader UK technology sector. This impact would be especially pronounced for UK technology companies with overseas customers.

VIII. Conclusion

49. Thank you for the opportunity to submit written evidence on the Draft Bill. If we can be of further assistance, please do not hesitate to contact us.

Joseph Lorenzo Hall
/s/
Chief Technologist [joe@cdt.org]

---

[30] RIPA, § 12 http://www.legislation.gov.uk/ukpga/2000/23/section/12

[31] Draft Bill Guidance notes, page 29.

Sarah St.Vincent
/s/
Human Rights and Surveillance Fellow [sstvincent@cdt.org]

Scott Craig
/s/
Ford/Mozilla Technical Exchange Fellow [scraig@cdt.org]