KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

David Anderson QC
Independent Reviewer of Terrorism Legislation
Brick Court Chambers
7-8 Essex Street
London
WC2R 3LD

Re: Evidence for Investigatory Powers Review

10 October 2014

Dear Mr Anderson

1. The Center for Democracy & Technology ('CDT') is pleased to submit this written evidence as part of the Investigatory Powers Review concerning Part 1 of the Regulation of Investigatory Powers Act ('RIPA') 2000, as amended by the Data Retention and Investigatory Powers ('DRIP') Act 2014.

2. CDT 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 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. Whilst based in Washington, DC, CDT also has a presence in London and Brussels.

Introduction and recommendations

3. Our evidence addresses three major aspects of RIPA (as amended) that, in our view, fail to comply with customary international law or the European Convention on Human Rights ('ECHR'). We have also highlighted some relevant aspects of US law governing surveillance in criminal cases for comparative or illustrative purposes.

4. Part I of our evidence assesses Section 4 of the DRIP Act, which empowers the Secretary of State for the Home Department to issue interception warrants that are intended to have extraterritorial effects; we conclude that such warrants, if issued, would violate customary international laws pertaining to state sovereignty and would also—at least in the United States—compel telecommunications service providers to violate local law. Parts II and III then address two features of the RIPA/DRIP regime that are incompatible with

Article 8 of the ECHR: the authorities' power to engage in potentially unlimited collection and storage of communications data under Chapter II of RIPA, and the Secretary of State's virtually unfettered power to issue retention notices under Section 1 of the DRIP Act. In the context of retention notices, we describe the US system of data preservation orders, which we believe adhere more closely to human-rights principles.

5. **We respectfully suggest that your recommendations should include the following:**

   - **Parliament should immediately repeal the extraterritorial provisions of Part I of RIPA (as amended by Section 4 of the DRIP Act), on the basis that they violate the UK's binding obligations under customary international law.**

   - **In the interim, the Secretary of State should refrain from issuing any extraterritorial interception warrants in order to avoid a violation of binding customary obligations (and avoid compelling telecommunications service providers to violate other States' domestic laws).**

   - **Parliament should mandate that when the Secretary of State believes the interception of communications outside of the UK's territorial jurisdiction is necessary and proportionate in the context of UK investigations or proceedings, she must adhere to the processes set out in mutual legal assistance agreements or other international agreements, or otherwise pursue disclosures through formal diplomatic channels.**

   - **If the Secretary of State retains the ability to issue extraterritorial interception warrants, primary or secondary legislation should provide that such warrants cannot compel disclosures that are not permitted by local law.**

   - **Parliament should adopt legislation requiring that authorisations or notices for obtaining or disclosing communications data (including under Section 8(4) warrants) be restricted to data concerning a single person or set of premises.**

   - **The legislation should also restrict the grounds on which the authorities may access communications data to those grounds that are strictly necessary for safeguarding the UK's democratic institutions (to include the protection of public safety and the prevention of serious crime).**

   - **Parliament should repeal Section 1 of the DRIP Act and replace the Secretary of State's power to issue data retention orders with a power for law-enforcement officials to issue data *preservation* orders that relate to individual users' data, where that data is required for specific investigations or proceedings.**

   - **If the Secretary of State retains the ability to issue data retention orders, Parliament should amend RIPA and the DRIP Act to provide that these orders are only valid with respect to data stored within the territorial jurisdiction of the UK, that the orders may only require the retention of the communications data of a specific individual named in the order and that they cannot be issued unless the**

retention is necessary and proportionate with respect to the individual in question.

6. Like RIPA, this submission uses the term 'communications data' to refer to data describing a communication, such as its sender, recipient, date, time, location and duration. The term 'interception' refers to the collection of the content of a communication.

I. Section 4 of the DRIP Act violates binding customary international law norms and would compel US telecommunications service providers to violate US law

7. In our view, insofar as Section 4 of the DRIP Act purports to empower the Secretary of State to issue interception warrants that would impose an obligation upon persons outside of UK territory, the legislation violates customary international law and should be repealed.

8. Customary international law is binding upon the UK[1], and one of the best-established rules found in that body of law is that in the absence of a permissive international-law norm to the contrary, a State '*may not exercise its power in any form in the territory of another State.*'[2] As a corollary of this rule, '*[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.*'[3]

9. Thus, any attempt by the UK to enforce an interception warrant in another State's territory would violate the binding customary rule of territorial sovereignty and constitute a serious breach of the international order.

10. One reason this customary norm is of critical importance is that a warrant or order compelling action in another State could force an individual or company to violate the domestic law of that State. Such a development could have serious implications for international relations and raises concerns about a lack of due regard for the international-law principle of comity.[4]

---

[1] *See Jones, R. v* [2006] UKHL 16 (29 March 2006), ¶ 11 (Lord Bingham).

[2] *S.S. 'Lotus'*, Permanent Court of International Justice, Judgment, Series A, No 10 (7 September 1927), p. 18; *see also Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, International Court of Justice, Judgment (Merits) (27 June 1986), ¶ 205 (finding that the customary principle of territorial and political integrity '*forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States*').

[3] Restatement (Third) of Foreign Relations, § 432(2), including comments (b)-(c) and list of sources.

[4] *See generally Viking Line ABP v International Transport Workers' Federation & Anor* [2005] EWHC 1222 (Comm) (16 June 2005). We understand the principle of comity to include not only concerns related to the jurisdiction to adjudicate, but also to the jurisdiction to prescribe (or issue judicial or administrative orders): *see Hilton v Guyot*, 159 U.S. 113, 163-164 (1895) (describing comity as '*the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons was are under the protection of its laws*'). *See also Hartford Fire Ins Co v California*, 509 U.S. 764 (1993) (discussing, in relation to comity, the relevance of the existence of a conflict between US and UK law).

11. For example, in the United States, the Electronic Communications Privacy Act ('ECPA') prohibits communications service providers from disclosing the content of an electronic communication within the first 180 days of the provider's storage of the communication, except pursuant to a warrant issued by a US judge or magistrate; this requirement applies regardless of the nationality of the communication's sender or recipient.[5] Moreover, a US federal appellate court (the Sixth Circuit Court of Appeals, whose rulings are binding within several US states and serve as persuasive authority in the other federal judicial jurisdictions) has found that under the Fourth Amendment to the US Constitution, a warrant is required even for content that is over 180 days old.[6]

12. In other words, at least within the Sixth Circuit, communications service providers cannot legally disclose communications content in the absence of a warrant issued by a US judge or magistrate based on a finding of probable cause. In our experience, providers in the US generally follow this Sixth Circuit ruling on a nationwide basis.

13. The DRIP Act, however, purports to require communications service providers in the US to disclose communications content without having first been served with a US judicial warrant based on a finding of probable cause. This requirement contradicts both ECPA and the US Constitution.

14. We are aware that as amended by the DRIP Act, RIPA seeks to impose an extraterritorial duty to give effect to a UK interception warrant only when it is '*reasonably practicable*' for the recipient to take the steps necessary to give the warrant such effect. In determining whether the steps a foreign entity must take are 'reasonably practicable', the DRIP Act provides that '*regard is to be had*' to the requirements of local law and the extent to which the interception warrant may be given effect without breaching that law.

15. We view this non-binding consideration as wholly inadequate to preserve the sovereignty interest that States have in controlling the execution of searches within their borders.

16. For all of the foregoing reasons, we respectfully recommend that Parliament repeal the extraterritorial provisions of Part I of RIPA as amended by Section 4 of the DRIP Act. If Parliament declines to do so, we respectfully recommend the adoption of either primary or secondary legislation providing that extraterritorial interception warrants cannot compel disclosures that are not permitted by local law.

17. For the same reasons, we recommend that Parliament require the Secretary of State to adhere to the processes set out in mutual legal assistance agreements or other relevant international agreements, or otherwise pursue formal diplomatic channels, when she believes that the interception of communications outside of the UK's territorial jurisdiction is necessary and proportionate in the context of investigations or proceedings within the UK.

---

[5] 18 U.S.C. § 2703(a).

[6] *US v Warshak*, 631 F.3d 266 (2010). The Fourth Amendment to the US Constitution establishes '*[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*'.

II. The authorities' exceedingly broad discretion to obtain communications data violates Article 8 of the ECHR

18. In our view, both the power to access communications data under Chapter II of Part I of RIPA and the virtually unfettered power to collect and use communications data obtained by way of interception warrants pursuant to section 5(6)(b) of RIPA are incompatible with the requirements of Article 8 of the ECHR.

19. As a general matter, the term 'communications data' includes 'the "who", "when" and "where" of a communication', whilst excluding the content of the correspondence.[7] It includes traffic data, service use and subscriber data.

20. We note that both individually and in the aggregate, communications data can reveal any number of intimate aspects of an individual's life, ranging from personal relationships to religious beliefs; sexual orientation; social, professional, educational and recreational activities; consultations with medical and legal professionals; reading habits; political activity; travel; and so on. As the Court of Justice of the EU ('CJEU') has observed in its judgment in *Digital Rights Ireland*, these data are particularly revealing when taken together and '*may allow very precise conclusions to be drawn concerning … private lives*'.[8] In some cases, the aggregation of such data may provide as complete a profile of an individual as the content of the communications would have done.

a. Article 8's requirements concerning communications data

21. Article 8 of the ECHR (taken together with Article 1) establishes that everyone within the UK's jurisdiction has the right to respect for his or her private life and correspondence, and that the UK public authorities are barred from interfering with this right except where such interference is both '*in accordance with the law*' and '*necessary in a democratic society*' in order to achieve certain legitimate aims.

22. As an initial matter, we recall the finding of the European Court of Human Rights ('ECtHR') that any public authority's collection of e-mail or telephone correspondence, or personal information pertaining to Internet usage, constitutes an interference with the right to respect for private life under Article 8.[9]

23. We further recall the Court's conclusion in *Malone v the United Kingdom* that an authority's collection of telephone communications data without the consent of the telephone subscriber also constitutes an interference under Article 8, as this data is an '*integral element*' of the correspondence.[10]

---

[7] 'Related communications data' for the purposes of Chapter I of Part 1 is defined under Section 20, while 'communications data' for the purposes of Chapter II is set out in Section 21(4)-(6). *See also* Home Office, Acquisition and Disclosure of Communications Data Code of Practice, ¶ 2.13 (hereinafter 'Code of Practice').

[8] *Digital Rights Ireland* (Judgment) [2014] EUECJ C-293/12 (8 April 2014), ¶ 27.

[9] *Copland v the United Kingdom* (2007), ¶¶ 43-44; *Liberty and others v the United Kingdom* (2008), ¶ 56.

[10] *Malone v the United Kingdom* (Plenary, 1984), ¶ 84; *see also PG and JH v the United Kingdom* (2001), ¶ 42; *Copland*, *supra* n. 9, ¶ 43.

24. It is clear, moreover, that the Court's finding concerning telephone communications data necessarily extends to data relating to such electronic communications as e-mail and general Internet usage. In other words, the requirements of Article 8 apply to the collection of electronic communications data just as they do to the interception of the content of correspondence. The recent CJEU judgment in *Digital Rights Ireland*, which found that the retention of communications data '*directly and specifically affects private life*' for the purposes of the Charter of Fundamental Rights of the EU, supports this view.[11]

25. The ECtHR's case-law has firmly established that in order for the UK to conduct secret communications-surveillance measures '*in accordance with the law*' for the purposes of Article 8, the public authorities must undertake those measures on the basis of a binding and publicly-accessible statutory law.[12] That law '*must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data*'.[13]

26. Moreover, the statutory law must set out, *inter alia*, '*the grounds required for ordering*' secret-surveillance measures.[14] Although the issuance of a surveillance order may involve some exercise of discretion on the part of the authorities, this discretion cannot be unfettered: '*the law must indicate the scope of any such discretion … and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*'.[15] Thus, a law that '*defines precisely, and thereby limits, the purposes*' for which the authorities are permitted to undertake the surveillance may meet Article 8's requirements.[16] By contrast, a law that does not clearly restrict and explain the scope of the executive's discretion, and particularly one whose list of possible grounds for surveillance is not exclusive, will not be compatible with Article 8.[17]

b. Application of Article 8's requirements to communications data under Part 1 of RIPA

27. We note that a warrant for the interception of '*external communications*' under Section 8(4) of RIPA, unlike an interception warrant under Section 8(1), does not contain any requirement that the warrant be targeted at a particular person or premises. We note further that a

---

[11] *Digital Rights Ireland*, *supra* n. 8, ¶¶ 26-29.

[12] *E.g.*, *Malone*, *supra* n. 10, ¶ 87; *Shimovolos v Russia* (2011), ¶ 68; *Weber and Saravia v Germany* (Decision, 2006), ¶ 95; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* (2007), ¶ 76.

[13] *Shimovolos*, *supra* n. 12, ¶ 68; *Liberty and others*, *supra* n. 9, ¶ 62; *Weber and Saravia*, *supra* n. 12, ¶ 93.

[14] *E.g.*, *Shimovolos*, *supra* n. 12, ¶ 68; *Liberty and others*, *supra* n. 9, ¶ 62.

[15] *Malone*, *supra* n. 10, ¶ 68; *Liberty and others*, *supra* n. 9, ¶¶ 64-70.

[16] *Klass and others v Germany* (Plenary, 1978), ¶ 45.

[17] *See Malone*, *supra* n. 10, ¶¶ 71-80; *Liberty and others*, *supra* n. 9, ¶ 64.

warrant to intercept communications also authorises '*conduct for obtaining related communications data*' (section 5(6)(b)).

28. In respect of the power to access communications data under Chapter II of RIPA, we note that the purposes for which the designated UK authorities may obtain this data are both broad and numerous. Additionally, the designated authorities are not required to restrict their collection of communications data to items concerning any specific person or set of premises, or to destroy the data if its storage becomes disproportionate or unnecessary.

29. Section 22(2) of RIPA, as amended by Section 3 of the DRIP Act, allows the designated authorities to obtain and disclose communications data where such action is '*necessary*':

    (a) in the interests of national security;
    (b) for the purpose of preventing or detecting crime or of preventing disorder;
    (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
    (d) in the interests of public safety;
    (e) for the purpose of protecting public health;
    (f) for the purpose of collecting or assessing any tax, duty, levy [etc.] payable to a government department;
    (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating [such injury or damage]; or
    (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

30. The Secretary of State has previously made several additions to this list via the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006, and we observe that RIPA empowers her to make further additions in future.[18]

31. As with the power to intercept external communications under Section 8(4), Chapter II of RIPA does not require that an authorisation or notice for the collection of communications data be restricted to data concerning a specific person or set of premises. Instead, with only a few exceptions, Sections 22(1) and 23 of RIPA permit the designated authorities to collect '*any communications data*' from any current, historic or future time period, so long as the authorities believe the collection of that data is 'necessary' for any one of the purposes set out in Section 22(2) and is proportionate to the aim pursued.[19]

32. Thus, the power to obtain communications data from bulk interception under Section 8(4) warrants, taken together with the broad scope of access to communications data under Chapter II, grants the UK authorities an extremely wide scope of discretion to obtain and store any type or volume of communications data, pertaining to any individual or class of individuals (or, indeed, entire communities or nations), from any time period, for one of any

[18] Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006, SI 2006/1878.

[19] Code of Practice, *supra* n. 7, ¶ 3.5. There are some restraints on the type of communications data that the designated authorities can collect in the interests of public safety, for the purpose of protecting public health or for tax-related purposes; see ¶ 2.4 of the Code.

number of broad and ultimately non-exclusive purposes. In effect, with very few exceptions, the legislation empowers the authorities to obtain any type or amount of communications data they like and store that data forever.

33. In this respect, the powers granted under Part I closely resemble those that were at issue in *Liberty v the United Kingdom*, and which the ECtHR struck down as incompatible with Article 8.[20] Furthermore, the Part I regime lacks the limitations on the scope of collection, and the duration of storage, that were essential to the Court's decision to uphold RIPA's provisions pertaining to interception warrants for internal communications in *Kennedy v the United Kingdom*.[21]

34. It is therefore our view that the Part I regime violates Article 8, and that Parliament should amend the legislation so as to:
    - Restrict the scope of collection of communications data obtained under Section 8(4) warrants to correspond with the targeting required of warrants under Section 8(1);
    - Require that authorisations or notices for the collection or disclosure of communications data specify a single individual or set of premises to which that data must pertain (whilst defining 'premises' in a manner that precludes indiscriminate collection or disclosure);
    - Require the destruction of communications data whose continued storage is not necessary or proportionate; and
    - Restrict the grounds upon which the surveillance of communications data is available to those that are '*strictly necessary for safeguarding*' the UK's democratic institutions (to include the protection of public safety and the prevention of serious crime).[22]

III. The Secretary of State's virtually unlimited power to issue data retention orders violates Article 8 of the ECHR

35. Finally, we submit that the Secretary of State's powers under Section 1 of the DRIP Act to issue data retention orders that are not subject to any statutory limitations as to scale or scope, for up to 12 months, on any of the broad grounds found in Section 22(2) of RIPA, violate Article 8 of the ECHR.

---

[20] *Liberty and others*, *supra* n. 9, ¶¶ 64-70. Concerning the storage of data, see *Segerstedt-Wiberg and others v Sweden* (2006), ¶¶ 87-92.

[21] *Kennedy v the United Kingdom* (2010), ¶¶ 160 (distinguishing *Kennedy* from *Liberty and others* on the basis that for the interception of internal communications, '*the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered*', such that '*[i]ndiscriminate capturing of vast amounts of communications is not permitted*'), 162 (further distinguishing *Kennedy* from *Liberty and others* on the basis that where the interception of internal communications is concerned, '*any captured data which are not necessary for any of the authorised purposes must be destroyed*'), 164 (also noting the requirement of destruction of unnecessary data, and noting the additional requirement that '*intercept material [concerning internal communications] must be reviewed at appropriate intervals to confirm that the justification for the retention remains valid*').

[22] *See Rotaru v Romania* (Grand Chamber, 2000), ¶ 47.

36. We observe that under Section 1 of the DRIP Act, the Secretary of State has the power to issue, at her discretion, a data retention order that applies to any public telecommunications operator or class of operator, and that requires the retention of *all* data (or any subset of data). Moreover, she may issue such an order pursuant to any of the grounds set out in Section 22(2) of RIPA, including such additional grounds as she herself may establish via an order pursuant to Section 22(2)(h). Under the DRIP Act and the relevant provisions of RIPA, the term 'public telecommunications operator' can include any entity that offers a telecommunications (i.e. electronic communications) service to any substantial part of the public anywhere in the UK.

37. In other words, the Secretary of State may use any one of the broad and numerous grounds listed in Section 22(2) of RIPA for ordering virtually any provider of electronic communications services, from a local or national Internet service provider (such as British Telecom) to transnational companies such as Google, T-Mobile and Vodafone, to retain *all* communications data that it transmits or generates.

38. Even assuming that such a retention order would not have any validity outside of the UK's territorial jurisdiction (see the discussion at Part I above), the DRIP Act thus empowers the Secretary of State to order the indiscriminate retention of the communications data of the entire population of the United Kingdom.

39. The ECtHR has repeatedly made clear that the retention (or storage) of personal data constitutes an interference with the right to privacy, and must be necessary in a democratic society and proportionate to a legitimate aim in order to withstand scrutiny under Article 8.[23] In this context, the Court has specifically emphasised the requirement in its case-law that '*powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions*', and has closely examined whether the retention of data pertaining to an individual could '*be deemed to correspond to any actual relevant national security interests*'.[24]

40. The Court has also specifically emphasised that retention, as an interference with the right to private life, cannot be arbitrary if it is to comply with Article 8.[25]

41. In this respect, we note the CJEU's judgment in *Digital Rights Ireland* (see paragraph 20 above), in which the Court struck down the Data Retention Directive as violating fundamental privacy rights equivalent to those found in Article 8 of the ECHR. Part of the basis for the CJEU's decision was the fact that the Directive mandated the indiscriminate retention of communications data—including of individuals '*for whom there [was] no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime*'.[26]

---

[23] *E.g.*, *Leander v Sweden* (1987), ¶ 48; *Segerstedt-Wiberg and others*, *supra* n. 20, ¶ 73; *Rotaru*, *supra* n. 22, ¶ 46.

[24] *Segerstedt-Wiberg and others*, *supra* n. 20, ¶¶ 88, 90; *see also Rotaru*, *supra* n. 22, ¶ 47; *Klass and others*, *supra* n. 16, ¶ 42.

[25] *Ibid.* at ¶ 76.

[26] *Digital Rights Ireland*, *supra* n. 8, ¶ 58.

42. We therefore conclude that the power the DRIP Act confers upon the Secretary of State to issue indiscriminate (or otherwise non-individualised) data retention mandates constitutes a clear violation of Article 8 of the Convention, and that at minimum, Parliament should amend the legislation to provide that:
    - Any data retention order issued by the Secretary of State or her agents will only be valid with respect to data stored within the territorial jurisdiction of the UK (see Part I above);
    - The retention order may only require the retention of the communications data of a specific individual who is named in the order (as in a system of data preservation orders—see below), and the retention of whose data is strictly necessary in order to achieve one of the aims set out in Article 8; and
    - The order may only seek the retention of data of a type and amount that are proportionate to this aim.

43. We reiterate that these are the *minimum* changes to Section 1 of the DRIP Act (and related provisions of DRIP and RIPA) that Article 8 of the ECHR requires.

44. In order to ensure that interferences with privacy do not exceed what is necessary and proportionate, CDT has long urged national governments to adopt a regime of data preservation orders instead of data retention orders. Data preservation orders, which are used in the United States and (as CDT research in 2012 indicated) Japan, are issued by law-enforcement officials and require communications service providers to preserve data that is relevant to a specific investigation or proceeding.[27] In the United States, statutory law obligates communications service providers to preserve a user's data upon the request of a governmental entity pending the issuance of a court order or other process that compels disclosure.[28] Pursuant to the request, providers must preserve the relevant records for a 90-day period, which is renewable.[29]

45. These data *preservation* orders interfere with the privacy of only a small number of individuals, and do so in a targeted manner that is easily capable of meeting the necessity and proportionality (or non-arbitrariness) requirements found in the privacy provisions of international human-rights instruments. The UK's data *retention* orders, by contrast, could interfere with the privacy rights of many or all users of a provider's services and therefore run a much greater risk of being unnecessary or disproportionate.

46. We observe that the United States Congress has thus far declined to enact legislation permitting the issuance of data retention mandates, and that members of Congress have cited civil-liberties concerns in opposing draft legislation that would have created such mandates.[30] We encourage the UK Parliament to take a similar stance and uphold

---

[27] Center for Democracy & Technology, 'Introduction to Data Retention Mandates' (September 2012), *available at* https://www.cdt.org/files/pdfs/CDT_Data_Retention-Five_Pager.pdf.

[28] 18 U.S.C. § 2703(f)(1).

[29] 18 U.S.C. § 2703(f)(2).

[30] Greg Nojeim, 'Data Retention Hearing: Opposition from Both Sides' (13 July 2011), *available at* https://cdt.org/blog/data-retention-hearing-opposition-from-both-sides/; Mark Stanley, 'How the Data Retention Bill Impacts You – And What You Can Do About It' (27 February 2012), *available at* https://cdt.org/blog/how-the-data-retention-bill-impacts-you-—-and-what-you-can-do-about-it/.

fundamental rights by adopting a system of individualised data preservation orders rather than sweeping data retention mandates.

* * *

47. We hope this evidence will assist you as you undertake your review. Please do not hesitate to contact us if we can be of further assistance.

Yours sincerely,

Sarah St Vincent
Human Rights and Surveillance Legal Fellow
Center for Democracy & Technology