KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

The Rt Hon Keith Vaz MP
Chair
Home Affairs Committee
House of Commons
7 Millbank
London
SW1P 3JA

Re: Comments on Part 3 of the draft Counter-Terrorism and Security Bill

15 December 2014

Dear Mr Vaz

1. The Center for Democracy & Technology ('CDT') thanks the Home Affairs Committee for this opportunity to submit our comments on the compliance of certain aspects of Part 3 of the draft Counter-Terrorism and Security ('CTS') Bill with the United Kingdom's obligations under the European Convention on Human Rights ('ECHR') and the Charter of Fundamental Rights of the European Union. We are further concerned about a number of aspects of Part 5 of the draft bill, including Chapter 2, and plan to submit additional comments about the compliance of that part of the bill with the ECHR as well as fundamental democratic principles at a later date.

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.

3. Whilst based in Washington, DC, CDT also has a presence in London and Brussels. We have previously submitted evidence to the Independent Reviewer of Terrorism Legislation concerning the Data Retention and Investigatory Powers ('DRIP') Act 2014 and the Regulation of Investigatory Powers Act ('RIPA') 2000.[1]

[1] The evidence CDT submitted to the Independent Reviewer of Terrorism Legislation on 10 October 2014 concerning certain aspects of the DRIP Act 2014 and RIPA 2000 is available at https://cdt.org/insight/submission-of-evidence-to-uk-investigatory-powers-review/.

Introduction and recommendations

4. We are in agreement with the Home Secretary that the United Kingdom and all other democratic societies face a need to prevent terrorist violence.

5. However, we are submitting these comments in order to draw the Parliament's attention to Part 3 of the draft CTS Bill, which, in our view, fails to comply with the ECHR and the EU Charter of Fundamental Rights. In particular, we are gravely concerned that this part of the draft bill, if adopted, would be highly inconsistent with the Convention rights to respect for private life and correspondence (Article 8) and freedom of expression (Article 10). We have therefore concluded that the Home Secretary's statement that the bill is compatible with the ECHR is incorrect.[2]

6. As an organisation that focuses on upholding the enjoyment of human rights online, we are especially concerned about the compelled retention of communications data, government monitoring of Internet-based expression and the creation of intelligence or other government databases containing unnecessary or disproportionate personal information. Each of these intrusive activities would or may take place under this legislation.

7. At present, our comments are restricted to Part 3 of the draft bill, which would create an unprecedented system to track individuals' Internet usage and match their online activities to certain identifying information. However, we remain deeply troubled by a number of provisions found in Part 5 of the bill, including not only Chapter 1 but also Chapter 2, which would codify a government-run programme to tag individuals as 'vulnerable to being drawn into terrorism' and develop plans of action concerning them that are susceptible to a variety of abuses. We believe the provisions of Part 5 of the draft bill, if enacted, would violate a range of fundamental rights and abrogate some of the most basic tenets of democracy. We plan to address Part 5 of the draft bill in a forthcoming submission.

8. Our apprehensions about the draft CTS Bill's compatibility with the ECHR extend beyond the provisions mentioned above. At present, however, we wish to highlight the problems inherent in Part 3 in line with our unique expertise.

9. **In light of our conclusions, our recommendations are as follows:**

   - **We recommend that Parliament abandon the scheme found in Part 3 of the draft bill, which would compel the retention of highly sensitive data concerning individuals' Internet usage and facilitate the linking of all such data with specific and identifiable persons. We are gravely concerned that the retention of this data, particularly (but not exclusively) if conducted in an indiscriminate fashion, would violate Article 8 of the ECHR as well as the right to the protection of personal data found in Article 8 of the EU Charter of Fundamental Rights.**

[2] See Home Office, 'Counter Terrorism and Security Bill: European Convention on Human Rights' (undated), available at http://www.parliament.uk/documents/joint-committees/human-rights/ECHR_Memo_Counter_terrorism_Bill.pdf.

- **Instead (as we have previously stated in our comments on the DRIP Act), we believe Parliament should replace the Home Secretary's power to issue data-retention orders under Part 3 with a power for law-enforcement officials to issue targeted data-preservation orders that relate to an individual user's data, where that data is required for specific investigations or proceedings.[3]**

I. Part 3 of the draft CTS Bill threatens privacy rights and should be rejected

10. Part 3 of the draft CTS Bill would enlist communication service providers ('CSPs') in a troubling 'IP-matching' surveillance program to enable the authorities to identify anyone involved in an Internet communication via UK networks and track their activities across online sessions.

11. CDT recognises the importance of ensuring that in specific cases involving suspected criminal offences, law-enforcement authorities have the ability to match Internet activity to a user's identity. We support the Home Office's stated goal of countering cybercrime and protecting vulnerable individuals, including children, from online victimisation and abuse.

12. However, we are concerned that Part 3 of the bill, as drafted, is so expansive as to violate the right to respect for private life and correspondence found in Article 8 of the ECHR as well as the right to the protection of personal data found in Article 8 of the EU Charter of Fundamental Rights. We are further concerned about the potential chilling effect of IP matching (as well as the other forms of data retention that the Home Secretary already has the power to order under the DRIP Act) on the freedom of expression found in Article 10 of the ECHR.

13. Part 3 of the draft bill contains data-retention provisions that would represent a significant increase in the surveillance powers the authorities currently possess under the DRIP Act and RIPA. As explained in the evidence we submitted to the Independent Reviewer of Terrorism Legislation in October 2014, the Home Secretary presently has the power under DRIP to order CSPs to retain, in bulk, a broad range of data concerning individuals' communications.[4] Part 3 of the draft CTS Bill would expand these powers even further by enabling the Home Secretary to compel CSPs to collect and retain data linking individuals to all dynamic IP addresses assigned to them when they use the Internet, so that the authorities may identify any person involved in an online communication via a UK network. The CSPs would be obligated to retain this data for up to 12 months, or (we believe) even longer if the relevant order is renewed.[5]

14. CDT has frequently commented on the unnecessary and potentially disproportionate risks to individual privacy rights posed by 'IP matching' and other user-identification proposals that

[3] We have previously made a similar recommendation concerning the data-retention provisions of the DRIP Act; see CDT's Evidence for the Investigatory Powers Review (*supra* n. 1).
[4] See *supra* n. 1.
[5] Data Retention and Investigatory Powers Act 2014, Section 1(5). The DRIP Act does not appear to place any limitations on the Home Secretary's ability to issue successive data-retention orders that may remain in force for up to 12 months each.

rely on data retention.[6] Dynamic matching of an individual Internet user to all of his or her IP address allocations in the course of a year (or even weeks or months) would allow the government and private companies to paint a detailed portrait of that individual's private life. The sheer quantity of information that may be gleaned from such logs, which comprise the sum of a person's online activities, is far greater than the information available through more traditional sources such as individual account billing records for telephone and Internet services. Further, much of this data will be highly sensitive, as a variety of highly personal activities and conversations that were once confined to private homes, law offices or physicians' surgeries have migrated to online platforms and services.

15. Internet users expect their CSPs to collect their sensitive information only as necessary in order to allow them to obtain access to online information and services, e-mail, other Internet-based communications platforms and personal data storage. Customers do not expect that their CSPs will create profiles linking their identifying information to the sum of their online activities and correspondence, and then retain those activity logs for months or years. As such, the IP matching component of the draft bill represents a significant threat to the right to privacy under Article 8 (which is outlined below) as well as other important freedoms. This bulk data-retention proposal may also conflict with the judgment of the Court of Justice of the EU in *Digital Rights Ireland*, which struck down the EU Data Retention Directive as violating the right to respect for private life and the right to the protection of personal data.[7]

16. We therefore urge Parliament to reject the 'IP matching' powers set out in Part 3 of the draft bill.

    a. *The draft CTS Bill would compel Internet companies to retain private customer data that they do not currently seek to store*

17. Without providing any technical explanation as to how its data-retention requirement would work, Part 3 of the draft bill would make CSPs responsible for recording identity, location and other user information each time they allocate an IP ('Internet Protocol') address to an individual device. The CSPs would then be required to retain that data for up to 12 months, or potentially even longer if the Home Office issues successive orders.[8] These data-retention requirements represent a significant extension of CSPs' current duties to monitor certain online activities that may be unlawful.

18. IP addresses, which are used to route traffic to devices and individual users on the Internet (much like a telephone number is used to route calls to a particular phone), are often assigned and re-assigned dynamically as they become available for use. This type of dynamic allocation allows Internet service providers and other CSPs to optimise the flow of

---

[6] See, e.g., Center for Democracy & Technology, 'DOJ Looking for Mandatory Internet Data Retention Law' (28 January 2011), https://cdt.org/blog/doj-looking-for-mandatory-internet-data-retention-law/; Center for Democracy & Technology, 'Data Retention Bill Is Dangerous Expansion of Government Power; Costly Mandate' (28 July 2011), https://cdt.org/press/data-retention-bill-is-dangerous-expansion-of-government-power-costly-mandate/; Mark Stanely, 'Victory for the Internet: Data Retention Mandate Absent from Bill' (6 July 2012), https://cdt.org/blog/victory-for-the-internet-data-retention-mandate-absent-from-bill/.

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

[8] See *supra* n. 5.

data traffic given that only a finite number of IP addresses exist. Systems do this by assigning and re-assigning unused IP addresses as network locations change, routers are reset or devices come online. An important aspect of dynamic allocation is that the user is not permanently associated with a particular IP address and may receive a different address at different times, and between different e-mailing or web browsing sessions.

19. In fact, the most recent version of the IP address standard—called 'IPv6'—originally used a particular device identifier (the network or 'MAC' address) as a portion of the IP address, but was subsequently modified so that a random number was chosen for this part of the address in order to mitigate privacy concerns. If this had not been done, each interaction with someone on the Internet would have exposed a globally unique device identifier to any party or eavesdropper to the connection. CSPs are therefore still able to provide a significant level of privacy for Internet traffic, and this method of using a randomly generated number as part of the IPv6 address is supported by all modern desktop and mobile operating systems.[9] Part 3 of the draft CTS Bill would fundamentally change this important feature of the Internet architecture and would roll back important privacy-preserving efforts to protect users from being identified unnecessarily.

20. 'IP matching' would thus be a radical extension of existing capabilities and not simply a technical update to data-retention laws.[10] It would change the delicate balance of the relationships between users, CSPs and the government in a manner that erodes individual privacy protections and may make it more difficult for CSPs to do business in the UK.

b. Part 3 of the draft bill permits indiscriminate mass surveillance of sensitive communications data and is disproportionate to the ends sought

21. We note that the Home Secretary has represented that IP matching is a 'targeted' process. However, we are concerned that characterising IP matching for individual users as a 'targeted' investigative technique misrepresents the impact of this mass identification programme.

22. Part 3 of the draft CTS Bill would amend the DRIP Act by adding IP addresses (and other online identifiers) to the types of data whose retention the Home Secretary may order pursuant to her powers under DRIP and RIPA. As we have pointed out in the evidence we submitted to the Independent Reviewer, Section 1 of the DRIP Act gives the Home Secretary the power to issue data-retention orders that apply to any CSP, and that require the retention of all data (or any subset thereof).[11] In other words, the DRIP Act allows the Home Secretary to order indiscriminate or 'dragnet' data retention. Part 3 of the draft CTS

---

[9] Alissa Cooper, 'Privacy in a Future that is Forever' (7 June 2012), https://cdt.org/blog/privacy-in-a-future-that-is-forever/.

[10] Under the DRIP Act, CSPs may be required to retain allocated IP addresses under some circumstances. However, as the Home Office has explained, there is presently 'no existing legal requirement for CSPs to keep a log of users and addresses', or to assist law-enforcement agencies 'to identify who was using an IP address at any particular time'. See Home Office, 'Counter-Terrorism and Security Bill: Factsheet – Part 3 – Internet Protocol (IP) Address Resolution' (undated), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/382367/CTS_Bill_-_Factsheet_5_-_IP_Resolution.pdf (hereinafter 'Home Office Factsheet').

[11] *Supra* n. 1.

Bill, as we understand it, would thus allow the Home Secretary to order the retention of IP-matching data in a manner that would not be 'targeted' in the sense of being limited to a specific individual or set of individuals.

23. Moreover, we note that (as suggested above) the kinds of data that would be subject to the data-retention scheme found in Part 3 of the draft bill could reveal any number of intimate aspects of an individual's life. These data, like other communications data whose retention the Home Secretary of State may order under DRIP, may reveal numerous details about an individual's private life even though they do not include the content of any conversations. For example, data concerning an individual's Internet behaviour can reveal personal relationships; 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 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.*'[12] 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.

24. This type of data retention has an impact on the privacy and expressive activities of all Internet users. As we have previously noted in the evidence we submitted to the Independent Reviewer, the European Court of Human Rights ('ECtHR') has repeatedly confirmed that the retention of personal data constitutes an interference with privacy rights, and must be necessary in a democratic society and proportionate to a legitimate aim in order to withstand scrutiny under Article 8 of the ECHR.[13] In this context, the Court has emphasised 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 sought to determine whether the retention of data pertaining to an individual '*correspond[s] to any actual relevant national security interests*'.[14] Every Internet user bears the impact of identification programs that match his or her name, identity and physical location to the sum of his or her online activities, and we submit that under the provisions the draft bill that permit such identification programs to operate in bulk or indiscriminately, that impact is disproportionate. The long-term retention of such identifying information also creates a risk of unlawfully inhibiting the freedom of expression (which is guaranteed in Article 10 of the ECHR).

25. We are aware of the Home Office's assurance Parliament that Part 3's 'provisions will be limited' with respect to user traffic and will not require CSPs to collect information regarding their customers' web-surfing habits by retaining the type of data it refers to as 'web logs', stating: 'Subsection (3)(c) specifically prevents a telecommunications operator providing an internet access service from retaining under this legislation data that explicitly identifies the internet communications service or websites a user of the service has accessed.'[15]

---

[12] *Digital Rights Ireland*, *supra* n. 7, ¶ 27.
[13] E.g., *Leander v Sweden* (1987), ¶ 48.
[14] *Rotaru v Romania* (Grand Chamber, 2000), ¶ 47; *Segerstedt-Wiberg and others v Sweden* (2006), ¶ 90.
[15] Home Office, Explanatory Notes to the Counter-Terrorism and Security Bill (26 Nov. 2014), available at http://www.publications.parliament.uk/pa/bills/cbill/2014-2015/0127/en/15127en.htm.

26. However, the restriction on the collection of 'web logs' is potentially misleading, as it could be read to suggest that users' web-surfing histories remain anonymous and inaccessible to investigators. Web logs are logs of the date, time, IP address, web address visited (a URL), information about the browser that visited the given URL and other information such as the user's preferred language. The precise extent of the 'IP log' contemplated by Part 3 of the draft CTS Bill is unclear, but at minimum this set of records would likely include the date, time and IP address of every visitor to a website. Some IP addresses correspond to one or very few possible web sites, and in these cases the distinction between a 'web log' and an IP log is immaterial: by knowing the IP address, one would necessarily also know the web site or communications service the user is accessing.

27. In other words, browsing anonymity is not, in fact, among the protections envisioned by the bill's drafters. In its own 'Factsheet' explaining IP matching, the Home Office acknowledges as much by stating that 'IP resolution would allow the police to trace the individuals who accessed' illegal content by demanding the IP log of all visitor traffic from the server hosting the website.[16]

28. Similarly, proposals to amend Part 3 with language protecting practitioners in specified 'sensitive professions' do not address many of the harms associated with mass surveillance of Internet traffic. Rather, these exceptions are instructive as to the concrete harms caused by mass surveillance. Journalists, media outlets, members of the legal profession and Parliamentarians are right to be troubled by the possibility that IP matching will expose their confidential, and sometime legally privileged, research and communications.[17] However, CDT believes this bill gives rise to serious privacy and free expression concerns on the part of all Internet users.

29. For these reasons, CDT submits, as it has done in previous comments to the Independent Reviewer of Terrorism Legislation, that Parliament should curtail the Home Secretary's power to issue data retention orders and replace it with a power for law-enforcement officials to issue targeted preservation orders that relate to an individual user's data, where that data is required for specific investigations or proceedings.[18]

II. Part 5, Chapter 2 of the draft bill undermines democracy and violates several fundamental rights enshrined in the ECHR

30. In our view, Part 5 of the draft bill, which (among other things) would require local authorities to establish panels tasked with assessing whether 'identified individuals' are 'vulnerable to being drawn into terrorism' and developing a plan of action accordingly, may fail to comply with several provisions of the ECHR and poses a serious risk to democratic principles in a number of respects.

31. We are particularly troubled by the possibility that police and other entities will seek to identify relevant individuals by actively monitoring social media, online discussions or other

[16] Home Office Factsheet, *supra* n. 10.
[17] Minutes of evidence taken before Joint Committee on Human Rights, Examination of witness David Anderson, QC (26 Nov. 2014), available at http://www.parliament.uk/documents/joint-committees/human-rights/Daivd_Anderson_Transcript_271114.pdf.
[18] *Supra* n. 1.

forms of lawful Internet-based interaction. We are also concerned about the possibility that police will seek to identify individuals as in need of 'support' by using secret surveillance under RIPA to obtain private communications data.

32. Moreover, we are disturbed by media reports suggesting that at least some of the 'support' activities that currently take place pursuant to the programme that Part 5, Chapter 2 of the draft bill would codify are in fact conducted for surveillance purposes, and that the names of people who are referred into the programme (along with exceptionally sensitive personal information such as their mental health and sexual practices) are collected and stored in intelligence databases.[19]

33. We believe that these and other aspects of Part 5 of the draft bill may breach the Convention rights to respect for private life and correspondence (Article 8), freedom of expression (Article 10), freedom of association (Article 11) and freedom of thought and opinion (Articles 9 and 10). Moreover, we are concerned that the violation of some of these rights may entail discrimination barred by Article 14.

34. We plan to discuss our apprehensions in these respects in a future submission; in the interim, however, we stand ready to provide any further information or analysis that would assist the Parliament at this juncture.

* * *

35. We hope these comments will assist the Home Affairs Committee, and we respectfully urge the Committee to consider our recommendations. Please do not hesitate to contact us (sstvincent@cdt.org or rcant@cdt.org) if you have any questions.

Yours sincerely,

Rita Cant
Free Expression Legal Fellow
Center for Democracy & Technology

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

[19] Nafeez Mosaddeq Ahmed, 'UK's flawed counter-terrorism strategy', *Le Monde diplomatique* (Dec. 2013), http://mondediplo.com/blogs/uk-s-flawed-counter-terrorism-strategy; Vikram Dodd, 'Government anti-terrorism strategy "spies" on innocent', *The Guardian* (16 Oct. 2009), http://www.theguardian.com/uk/2009/oct/16/anti-terrorism-strategy-spies-innocents.