Written evidence submitted by Dr Nora Ni Loideain
Technology and Democracy Project
University of Cambridge

I submit this evidence in my capacity as a Postdoctoral Research Associate for the Technology and Democracy Project within the Centre for Research in the Arts, Social Sciences and Humanities (CRASSH) at the University of Cambridge. Prior to completing my PhD in law on the right to privacy and the mass retention of communications data under EU law at the University of Cambridge, I was a Legal and Policy Officer for the Office of the Director of Public Prosecutions of Ireland and clerked for the Irish Supreme Court.

This evidence is offered in response to the call for submissions regarding the revised Investigatory Powers Bill and provides some recommendations for the consideration of the Public Bill Committee concerning:

- Scope of retention and access to Internet Connection Records
- Technical Capability Notices and human rights compliance
- Adequate and Sufficient Resources for the Investigatory Powers Commissioner
- Post-Legislative Scrutiny of Investigatory Powers Bill

1. Scope of retention and access to Internet Connection Records

1.1. The Joint Committee on the draft Investigatory Powers Bill should be commended for highlighting in their report the wide scope of information that Internet Connection Records (website browsing history) can actually reveal about a person's private life.[1] While Internet Connection Records (ICRs), a novel and much-criticised technical concept introduced by the Government in the draft Bill[2], do not provide a full website history (ICRs would provide a history of every website you visit but not every page), they still reveal a considerable amount of personal data. Through

[1] The definition of ICRs was first introduced under clause 47(6) of the draft Investigatory Powers Bill and has since been the subject of very minor revision under clause 54(6) of the Bill.
[2] For further on the issues concerning the lack of clarity and uncertainty surrounding the ICRs regime, please see the following presentations by a panel of legal and computer engineering experts hosted by the Technology and Democracy Project in February 2016: http://sms.cam.ac.uk/media/2186709.

intruding on a person's privacy to read online, these records can identify very sensitive information such as your financial status (nationaldebtline.org) or concerns regarding your, or a relative's or friend's, health (cancerresearchuk.org, samaritans.org). Accordingly, the Joint Committee found that the description of ICRs as being "simply the modern equivalent of an itemised phone directory" is "not a helpful one".[3]

1.2 On the basis that this information is not considered to constitute content, ICRs fall under the category of "communications data" which cover types of information consequently accorded a lower level of safeguards and oversight. Hence, under the revised Bill, access to the content of an e-mail requires a warrant whereas access to *who* you e-mail, *when* you e-mail them and *how often* (described as "entity" and "event" data under the IP Bill) only requires the authorisation of a designated senior person within the public authority seeking the communications data/ICRs.

1.3 However, the specific type of information that ICRs can reveal does not sit neatly within the 'content/context' distinction that provides the justification for the lower level of safeguards being applied to the authorisation and access to ICRs under the IP Bill. In other words, ICRs are providing more information about a person's private life than just the *context* of their communications, e.g. where and when a person uses the Internet. The information revealed by having access to ICRs goes much further because the *content* of what a person's is accessing over the Internet is revealed, e.g. websites that indicate their political views, the state of their health and finances and other sensitive personal data.

1.4 Furthermore, the long-term retention of this information over the duration of 12 months[4] will make it possible to construct a comprehensive profile of a person from the aggregation of what is likely to be at least 70, 000 ICRs.[5] This narrative data becomes consistently more detailed on a daily basis based on the ICRs automatically

[3] Joint Committee Report on the Draft Investigatory Powers Bill, para 126.
[4] Clause 78(3) of the revised Bill.
[5] This estimate is based on a request by a German Green Party representative to his CSP for the number of communications data collected and retained from the use of his mobile phone over a six-month period (35, 000 records): M. Spitz, "Your Phone Company is Watching You" TEDGlobal, Edinburgh, June 2012.

generated from every time a person's uses the Internet over their smartphone, tablet and personal computer.

1.5 Regarding the necessity and proportionality of the indiscriminate retention of ICRs, the value to law enforcement having access to such information has been outlined in some detail, e.g. identifying individuals involved in networks concerning terrorism or serious crime through tracking their online communications, such as fraud or drugs trafficking.[6] However, less consideration has been given to showing detailed evidence and reasons justifying the proposed mass and indiscriminate retention period of twelve months and the wide scope of access to be granted to many other public authorities. In other words, an evidence-based approach is lacking.

1.6 This raises not just questions of compatibility with the proportionality requirement mandated by the right to respect for private life as guaranteed under Article 8 of the European Convention on Human Rights (ECHR) and Article 7 of the EU Charter of Fundamental Rights but also raises concerns for data security, as protected under Article 8 of the EU Charter. As highlighted in the RUSI Report drawn on by the Government in its drafting of the IP Bill, the longer the data is held, the greater the risk that the data may be lost and/or stolen.[7]

1.7 The Operational Case policy document (revised following the pre-legislative scrutiny of the draft Bill) draws its recommendation for the 12-month retention period principally from the findings of only two studies. The first concerns the ability of law enforcement to investigate referrals made by National Centre for Missing and Exploited Children (NCMEC) involving an examination of 6025 referrals over a 9-month period. The second study concerns an analysis of the use of mobile devices in relation to approximately 600 suspects in serious crime investigations in order to show the prevalence of the use of online communications services by these individuals.[8]

---

[6] See the Operational Case for the Retention of Internet Connection Records and the Impact Assessment: Communications Data.
[7] *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (2015), para 5.52.
[8] Operational Case for the Retention of Internet Connection Records, pp.16-20.

1.8 No information is provided in the second study regarding over how long a time period these serious crime investigations took place. Furthermore, no references to findings based on the operation of similar laws in other jurisdictions have been included to support the proposed scope for this new surveillance power under the IP Bill.

1.9 It is also important to note that the focus of both of these studies, including the eleven case studies[9], all concern the investigation of serious crime. However, no detailed studies have been included to provide compelling evidence for the justification of allowing access to website browsing history spanning 12 months for the many other purposes under the IP Bill, such as tax assessment or protecting public health.[10]

1.10 The IP Bill provides that at least 46 public authorities (including the Food Safety Authority) will be authorised to access all types of communications data, including website browsing history (IP Bill, Schedule 4). Access to such long term website browsing history could identify an individual's personal and professional relationships, their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning their health or sex life.

1.11 Detailed studies may have been undertaken showing why all of these public authorities should be granted access to such an extensive amount of sensitive personal data. However, while a handful of anecdotal cases have been provided as examples, no comprehensive evidence has been made publicly available as yet. While these two studies and eleven anecdotal examples indicate that the retention of ICRs would be useful to law enforcement authorities, the indiscriminate retention of everyone's ICRs for a period of twelve months in case it may be needed has not yet been justified.

1.12 Notably, the Home Secretary was asked in Parliament on the publication of the draft IP Bill regarding what evidence resulted in the adoption of a 12-month retention period for communications data. Her response was that the Government had

[9] Of the eleven anecdotal examples, five concerned fraud, three involved child sexual exploitation, one involved drugs trafficking, one involved distribution of indecent imagery of children and one concerned organized immigration crime.
[10] Clause 46(7) of the revised Bill.

relied on the *Digital Rights Ireland* judgment (C-293/12 and C-594/12), delivered by the Grand Chamber of the Court of Justice of the EU (CJEU) in April 2014 that struck down the EU Data Retention Directive, as justification for this retention period.

1.13 However, the CJEU made no endorsement in its landmark digital privacy judgment for a 12-month period for the indiscriminate retention of communications data, or any specific period for that matter. Instead, the Luxembourg Court established that the determination any communications data retention period "must be based on objective criteria in order to ensure that it is limited to what is strictly necessary" (para 64). This requirement is based on the principles and conditions of Article 8 ECHR and Article 7 of the EU Charter of Fundamental Rights.

1.14 Hence, the compelling operational case for the current provisions of the IP Bill concerning its proposed scope for the mass and indiscriminate retention of website browsing history for 12 months, and its proposed accessibility to such a broad range of public authorities beyond the intelligence and police authorities, remains to be made. Accordingly, the compatibility of this aspect of the IP Bill with the proportionality requirement mandated by the right to respect for private life guaranteed under Article 8 ECHR and Article 7 of the EU Charter is suspect.

1.15 Indeed, the Grand Chamber of the Luxembourg Court will shortly deliver its judgment on this very issue in the Joined Cases of *Tele2 Sverige* (C-203/15) and *Davis* (Case C-698/15). It is significant to note that the President of the Court has already highlighted the importance of this preliminary ruling by granting an order to expedite the proceedings. Furthermore, the President has already determined that:

> [I]t is clear that national legislation that permits the retention of all electronic communications data and subsequent access to that data is liable to cause serious interference with the fundamental rights laid down in Articles 7 and 8 of the Charter.[11]

[11] Order of the President of the Court, Request for a preliminary ruling under Article 267 TFEU from the Court of Appeal (England and Wales) (Civil Division), 1 February 2016, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=174165&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=660741 .

Recommendations

On the basis that ICRs reveal the *content* of what a person has accessed via Internet usage (not just the context – where/when/how), public authorities should only be granted access to ICRs following the obtaining of a warrant. Hence, the authorisation regime that applies to the obtaining of ICRs should be amended and placed under the "Lawful Interception of Communications" as governed by Part 2 of the Investigatory Powers Bill.

Evidence should also be submitted to Parliament demonstrating the need for an indiscriminate twelve-month retention period that justifies the necessity and proportionality of such a major interference with the rights to private life and data protection of every person within the United Kingdom.

2. Technical Capability Notices

2.1 The Science and Technology Committee recommended that unencrypted information should only be sought from CSPs where such a request is "clearly feasible", "reasonable practicable" and "consistent with the right to privacy in UK and EU law".[12] The Government has stated that clauses 217 and 218 of the revised Bill have been amended in response to this recommendation.[13]

2.2 However, there is no explicit requirement for the Secretary of State to consider the legality, necessity and proportionality tests as mandated under the rights to respect for private life and the protection of personal data guaranteed by UK and EU law before issuing a technical capability notice in the revised Bill or in the relevant Draft Code of Practice (Interception of Communications).

2.3 Such an omission casts significant doubt over one of the key objectives of this proposed legislation to "strengthen safeguards and introduce world-leading oversight

[12] House of Commons Science and Technology Committee, *Investigatory Powers Bill: Technology Issues* (HC 573, 2016), para 42.
[13] *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny* (Cm 9219, 2016), p.92.

arrangements"[14] and fails to address a key area of concern for the ISC that "privacy protections should form the backbone" of the IP Bill.[15]

Recommendation

Clause 218(3)(e) of the revised Bill should be amended to state that the Secretary of State will consider "whether the interference with the rights to respect for private life and protection of personal data are justified in light of the legality, necessity and proportionality tests under the Human Rights Act and the EU Charter of Fundamental Rights".

Paragraph 8.10 of the Interception of Communications Draft Code of Practice should also be subject to the same amendment.

3. Adequate and Sufficient Resources for the Investigatory Powers Commissioner

3.1 The Government has promised that the proposed Investigatory Powers Commissioner will be adequately resourced. This commitment is paramount if the Commissioner is to be in a realistic position of effectively carrying out a growing number of detailed audits involving the technological and surveillance developments in everyday communications that are becoming ever more sophisticated.

3.2 One such example is the "Internet of Things" where more and more personal devices will become 'smart' (Internet enabled), resulting in the use of our possessions and homes being increasingly monitored for personal data, e.g. cars, houses, children's toys, wearable devices monitoring/managing serious health conditions.

3.3 Using a targeted equipment interference warrant, the Bill permits the intelligence agencies and law enforcement authorities to interfere with such devices for the purpose of countering threats to national security (clause 91) or to prevent or detect serious crime (clause 96). As highlighted in the Anderson Report, this technique, only recently made known to the public in February 2016, is effectively

[14] Draft Investigatory Powers Bill, p.5.
[15] ISC, *Report on the draft Investigatory Powers Bill*, para 9.

"hacking, in common parlance".[16]

3.4 Given that clause 96 is open to very wide interpretation and the recently avowed power of the intelligence agencies to acquire masses of such personal data in Bulk Personal Datasets (clause 174)[17], the use and impact of these powers on people's private life, their homes and the security of their personal data need to be subject to a high level of scrutiny and review.

3.5 Hence, it is submitted to the Committee that section 46 of the Counter-Terrorism and Security Act 2015 should be amended to ensure that the narrow remit of the Privacy and Civil Liberties Board should be expanded so that the Board may provide advice and assistance to the Investigatory Powers Commissioner in the oversight, auditing and review of the use and impact of the above powers and others under the Bill.

3.6 The Board could provide the necessary range of skills and expertise (e.g. former law enforcement and intelligence officials, forensic experts, computer scientists, lawyers, civil society, social media/communications experts, statisticians) that Ms Joanna Cavan, Head of the Interception of Communications Commissioner's Office (IOCCO) considers necessary to "ensure that the public authorities are robustly held to account and that all critical views are represented".[18]

3.7 Furthermore, the Board could alleviate a considerable administrative and resource burden from the many public authorities and CSPs affected by the Bill by systematically collecting and analysing the detailed statistical information essential for measuring the use and impact of the Bill's powers in the IPC's Annual Report (as required under clause 201).

---

[16] D. Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (2015), para 6.24.

[17] It was recently avowed that there is already a legal basis in place for the security and intelligence agencies to acquire and use bulk personal datasets under the Security Service Act 1989 and the Intelligence Services Act 1994.

[18] Head of the IOCCO, 2 November 2015, available at: http://iocco-uk.info/docs/Kings%20College%20Round%20Table.pdf .

3.8 Finally, the Board could also provide advice and assistance, in addition to statistical evidence, to the major review of the Bill by the specially constituted joint committee of the two Houses in the five years following the Bill's enactment.

Recommendation

It is recommended that the Counter-Terrorism and Security Act 2015 be amended to expand the narrow remit of the Privacy and Civil Liberties Board so that the Board may provide advice and assistance to the Investigatory Powers Commissioner, Judicial Commissioners and staff in the discharge of their functions.

4. Post-Legislative Scrutiny of Investigatory Powers Bill

4.1 In response to the Joint Committee on the Draft Investigatory Powers Bill Report, clause 201 of the revised Investigatory Powers Bill now provides that the annual report of the Investigatory Powers Commissioner will examine and include information on the results of the use of the powers under the Bill, *including its impact*. The report will then be published subject to material that may be removed if the Prime Minister is of the opinion that such information would not be in the public interest or for a number of other reasons, including the economic well-being of the UK.

4.2 This strengthening by the Government of the post-legislative scrutiny of the Bill is welcome, particularly the measurement of its impact as the relevant statistics should show how effective the Bill's powers have been in countering terrorism and serious crime.

4.3 Furthermore, these annual reports should establish whether the operation of the Bill's provisions have met the principles and safeguards of the legality, necessity and proportionality tests, as required under Article 8 ECHR and Articles 7 and 8 of the EU Charter of Fundamental Rights.

4.4 Although in light of clause 201, it is unclear what clause 222 (as currently drafted) will contribute in addition to that made by the annual reports of the Investigatory Powers Commissioner.

4.5 In its current form, clause 222 provides that the Secretary of State will prepare a report reviewing the operation of the Bill within six years of the law's implementation.

4.6 However, any contribution or recommendation by the Secretary of State concerning the Bill's operation will already have been incorporated into the Commissioner's Report on an annual basis during this six-year period. An alternative regime is therefore required and as the Joint Committee has observed:

> A provision which asked Parliament to revisit the intrusive powers it gives to the Executive after a period would, in our view, be a healthy way to fulfil the welcome aspirations for greater openness and legitimacy which underpin the draft Bill.[19]

Recommendation

It is recommended that clause 222 be amended to follow the original framework for post-legislative scrutiny put forward by the Joint Committee in its report.[20] Clause 222, as amended, would then provide that a specially constituted joint committee of the two Houses would review the Bill within six months of the end of the fifth year after the Bill is enacted.

[19] Joint Committee Report on the Draft Investigatory Powers Bill, para 708.
[20] Ibid, paras.709-710.