LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on 'Internet Connection Records' in the Investigatory Powers Bill for Report Stage in the House of Lords

October 2016

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Bella Sankey
Director of Policy
Direct Line: 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sara Ogilvie
Policy Officer
Direct Line: 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Silkie Carlo
Policy Officer (Technology & Surveillance)
Direct Line: 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

Sam Hawke
Policy Assistant
Direct Line
Email: samuelh@liberty-human-rights.org.uk

Summary

Liberty urges parliamentarians to oppose Government plans to force internet service providers to retain and store ‘internet connection records’ – the internet histories of every internet user in the UK – in order for them to be accessed by the police and intelligence agencies.

Internet connection records will decimate UK citizens’ rights to privacy and freedom online, with internet users browsing the web in the knowledge that their every online move is being logged and available to the eyes of the state.

The ‘ICR’ proposal is not only in conflict with fundamental human rights – it is a tried and failed policy that will not aid law enforcement, and that the intelligence agencies say they do not need. The regime will require potentially billions of pounds in public spending on private telecommunications companies, will endanger the cybersecurity of every internet user, and will have a chilling effect on the way our society uses the internet. No other Western democracy spies on the internet use of its citizens in this way.

As we begin to live more and more of our lives online, it has never been more important to uphold civil liberties in the digital context.

Contents

[1] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265

REMOVE 'INTERNET CONNECTION RECORDS'

New Clause

Internet Connection Records

(1) A retention notice must not require a telecommunications operator to retain "internet connection records".

(2) In this Act "internet connection record" means communications data which –

a. may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

b. comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

Effect

This new clause would explicitly prohibit retention notices being issued that force telecommunications operators to retain internet connection records.

Briefing

The change in legislation

The Bill describes a new category of information – an internet connection record – and provides significant new powers (a) for the Home Secretary to require telecommunications operators to generate and retain 'internet connection records' (ICRs) for up to 12 months and (b) for a multitude of public authorities to gain access to ICRs. The Data Retention and Investigatory Powers Act, 2014 allows for communications data to be retained that identifies the senders and recipients of communications online but specifically excluded the obligation to retain the most revealing data, previously described as 'web logs' but presented here as ICRs, that would explicitly identify the websites or internet communications services users have accessed.[2]

[2] *Counter Terrorism and Security Act 2015,* section 21(3)(c)

Extent of access to ICRs

A plethora of public authorities would have access to ICRs, including HMRC, the Department for Work and Pensions (and a range of other government departments), NHS Trusts, the Gambling Commission, the Food Standards Agency, and several ambulance services.[3] The scale of public authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access.

The recent IOCCO report revealed that in 2015: "***761,702 items*** *of communications data were acquired by public authorities during 2015. An item of data is a request for data on a single identifier or other descriptor, for example,* ***30 days of incoming and outgoing call data in relation to a mobile telephone would be counted as one item of data***."[4]

Making the population's internet histories also available to police for any investigative purpose will lead to unprecedented covert intrusion into potentially hundreds of thousands of peoples' private lives.

Unwarranted access to ICRs

Public authorities will not need a warrant to obtain an individual's detailed internet connection records. Applications by law enforcement and public authorities to acquire ICRs will mirror existing provisions for access to communications data and instead be authorised by a 'designated person'[5] within the public authority, and then by a 'single point of contact.'[6] Provisions in the Bill would permit law enforcement and public authorities to gain access to ICRs to reveal all the internet connections of a subject or subjects.[7]

Government amendment: no increased threshold for access to ICRs

The Labour Shadow Home Secretary, Andy Burnham MP, urged the Government for clearer definitions of ICRs. He also criticised the low threshold for access ICRs, writing to the former Home Secretary Theresa May:

> *I believe the threshold at which ICRs can be accessed must be higher. At present, the Bill sets it at any crime. I do not think it is necessary or proportionate for information held in ICRs to be accessed in connection with lower-level offences.*

---

[3] *Investigatory Powers Bill 2016,* schedule 4, part 1
[4] *Annual Report of the Interception of Communications Commissioner, 2015* – IOCCO, September 2016
[5] *Investigatory Powers Bill 2016,* clause 53
[6] *Investigatory Powers Bill 2016,* clause 67. A SPoC is an "*accredited*", "*trained*" individual. *Investigatory Powers Bill: Explanatory Notes,* 4 Nov 2015, p. 27
[7] *Investigatory Powers Bill 2016,* clause 54, subsection (4)

> *Instead, I think* ***this threshold should be set at serious crime and that this should be defined in the Bill as an offence that attracts a maximum sentence of not less than three years in prison****.*[8]

However, the Government responded with an amendment that in fact provides multiple routes for access to ICRs: to prevent or detect serious crime; to prevent or detect "other relevant crime" defined as any incurring a six month sentence; or to prevent or detect an offence involving "the sending of a communication".[9]

In the House of Lords Committee on the Bill, Lord Rosser described the Labour party's position:

> *(…) we have continuing concerns around the definition of "relevant crime", which we feel is too broad and could still lead to the use of ICRs in connection with crimes that would not be regarded as serious. (…)* ***We wish to see the wording in the government amendment tightened further.***[10]

ICRs are not the equivalent of a telephone call record

ICRs would provide a detailed record of internet connections for every person in the UK and comprise a 12 month log of websites visited, communications software used, system updates downloaded, desktop widgets used (e.g. calendars, notes), every mobile app used (e.g. Whatsapp, Signal, Google Maps), and logs of any other device connecting to the internet, such as games consoles, baby monitors, digital cameras and e-book readers.

The Government compares internet connection records to telephone records and asserts that expansion into internet records is merely filling a gap left by technological innovation. Similarly Baroness Harding, CEO of TalkTalk (one of the major ISPs to be reimbursed by the Home Office for generating ICRs), supported the policy during Second Reading of the Bill in the House of Lords claiming that "*Knowing what website someone visits is just the modern equivalent of knowing who they called*". However, such comparisons are deeply misleading. Call records show who telephoned who, where and when; internet connection records, by offline analogy, are more comparable to a compilation of call records, postal records, library records, study and research records, film and TV records, political and religious records, shopping records, social and leisure activity records, location records, and additionally capture concerns about health, sexual and family issues.

---

[8] *Letter to the Home Secretary on the Investigatory Powers Bill* – Andy Burnham MP, 4th April 2016, (emphasis added) http://andyburnhammp.blogspot.co.uk/2016/04/letter-to-home-secretary-on.html
[9] *Investigatory Powers Bill, 2016,* clause 59

The chilling effect of ICRs

Evidently, the proposal to store the internet records of every UK web user, with unwarranted access by police and bulk access by the Agencies, is an unprecedented breach of multiple human rights, particulalry freedom of expression and privacy.

Lord Paddick described a powerful example of the ways in which people might use the internet for deeply private matters, for example concerning sexuality, and considered whether people will refrain from seeking confidential advice on the internet in the knowledge that their every online move is being recorded. Privacy is a prerequisite for free personal development, and is essential online where many people now socialise, learn, research, express political opinions and share ideas. The sense of being watched online is certain to have a chilling effect on individuals' freedom, denying not only the personal rights of every citizen but hampering the freedom, education and growth of our society as a whole.

ICRs do not naturally exist

ICRs do not naturally exist within the technical infrastructure of a telecommunications operator. Under this Bill, telecommunications operators would be forced to make considerable infrastructural changes to generate and retain "ICRs" in bulk. Although there are a variety of ways in which authorities can obtain comparable data on a targeted basis, **there is no targeted method by which to generate "ICRs" – this is inherently a bulk power.** Correspondingly, the Agencies would be able to acquire this intrusive, population-level data in bulk under the terms in this Bill.

There is nothing on the face of the Bill to limit the potential data fields within ICRs. Rather, the Home Office describes the definition of ICRs as 'flexible',[11] and the draft Code of Practice confirms that 'there is no single set of data that constitutes an internet connection record'.[12] The Home Office was pressed to release further evidence to define what would be collected as 'communications data' including ICRs to the Joint Committee.

[11] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.1
[12] *Communications Data: Draft Code of Practice* – Home Office, 1 March 2016, p.18

It released an annex of 'examples' which revealed that the following fields of information are included in an internet connection record: [13]

- Websites visited
- Timestamp of each internet connection
- IP addresses
- Names
- Addresses
- Email addresses
- Telephone numbers
- Billing data
- Usernames
- Passwords
- Location data
- Unique device identifiers (MAC address, IMSI, IMEI)

Widespread concerns from major tech companies in response to the Home Office's ICRs proposals led the Committee to the damning recommendation that "*more effort should be made to reflect not only the policy aims but also the practical realities of how the internet works on a technical level.*"[14]

Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways.

Andy Burnham MP wrote to Theresa May that the ICR proposal "*goes beyond what is required by the Police and NCA"[15].*

As noted by Lord Paddick:

> *"**The security services MI5, MI6, and GCHQ say that they do not need internet connection records** because they can get the information they need by other means".*

Police can obtain this information by several means. Firstly, they can request telecommunications operators to retain the data of specific targets on a forward-looking basis[16], or they can conduct targeted interception.

---

[13] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.6
[14] Ibid. Recommendation 7, para. 122
[15] *Letter to the Home Secretary on the Investigatory Powers Bill* – Andy Burnham MP, 4th April 2016, http://andyburnhammp.blogspot.co.uk/2016/04/letter-to-home-secretary-on.html

Secondly, they can request retrospective 'internet connection' data on specific targets from operators who temporarily store it for their own business purposes.[17]

Thirdly, if they are seeking to prevent or detect serious crimes (such as child sex abuse, financial crime, drug smuggling, etc.) they can request data or assistance from GCHQ, which has a remit to provide intelligence for these purposes.[18] Intelligence sharing to tackle online child sexual exploitation will be fortified by the establishment of the NCA and GCHQ Joint Operations Cell (JOC), which was launched in November 2015[19]. The ISC noted that the delivery of ICR proposals:

> *"could be interpreted as being the only way in which Internet Connection records may be obtained.* ***However, this is misleading: the Agencies have told the Committee that they have a range of other capabilities which enable them to obtain equivalent data****."*[20]

The ISC recommended that this be amended in the Bill "*in the interests of transparency*"; yet no such transparency has been provided.

It is far more preferable, with regard to human rights, law enforcement, and public spending, to **employ robust targeted powers on identified suspects than intrude on the rights of the entire population.**

Some unconvincing attempts have been made to explain why existing powers, including using targeted interception, making targeted requests for communications data from service providers, and seizing and forensically examining a device, may sometimes be deemed less desirable than mass ICRs.

For example, it is claimed[21] that services such as Facebook may not hand over stored data unless police provide evidence that the individual in question definitely accessed their service.[22] This is entirely at odds with common practice – Facebook and other providers assist with law enforcement extensively. The arguments against using existing methods are wholly unconvincing and are far from justifying this mass surveillance regime of unprecedented intrusion and proven ineffectiveness.

---

[16] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.25
[17] *Operational Case for the Retention of Internet Connection Records,* 2015, p.25
[18] *The threat from serious crime* – GCHQ, 2015 http://www.gchq.gov.uk/what_we_do/the-threats-we-face/the-threat-from-serious-crime/Pages/index.aspx
[19] *GCHQ and NCA join forced to ensure no hiding place online for criminals* – NCA, 6 Nov 2015
[20] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation I (emphasis added).
[21] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4
[22] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4; p.25

Lord Oates remarked:

> *"That is not evidence-based policy-making; it is policy-based evidence making".*

Liberty believes the case supporting this expanded data collection is deeply flawed, contradicted by the available evidence, and has been accurately described as "*overstated and misunderstood*".[23]

There is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[24].

In fact, **David Anderson noted that:**

> **"*such obligations were not considered politically conceivable by my interlocutors in Germany, Canada or the US*",**

and therefore, "*a high degree of caution*" should be in order.[25] As the CJEU ruled in 2014,[26] the indiscriminate collection and storage of communications data is a disproportionate interference with citizens' right to privacy. It is unacceptable that Government is attempting to bypass this ruling, and to extend its policy of blanket data retention.

There is no case for the 'necessity' of ICRs

Mr Anderson's *Report on the Review of Bulk Powers* was published on 19th August 2016. Mr Anderson did not review the proposed new power to require the retention of "ICRs", as stated in paragraph 2.5(b).[27]

In oral evidence to the Joint Committee on the Draft Investigatory Powers Bill, on 2nd December 2015, Mr Anderson said:

> *They* (the Government) *have done what I recommended and made out an operational case as to the respects in which the police would find that useful.* ***Does that mean they are deliverable? Not necessarily.*** *I am not seeking to express a view on this, because I do not have one and I am not competent to have one, but* ***there are some serious questions there****. Another Committee, I know, is taking evidence on some of these*

[23] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[24] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[25] Ibid
[26] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014
[27] *Report of the Bulk Powers Review* – David Anderson Q.C., 19 August 2016, para 2.5(b), p.21

questions. Would it be technically feasible to assemble precisely the types of data that they say are wanted? Would it be operationally worthwhile? My understanding is that, although no other western country currently seeks to deliver internet connection records there was an attempt to do something very similar in Denmark. This happened until June 2014, when the law was repealed. One of the stated reasons for that is that the police had not found it as useful as they had hoped.[28]

The Government published its "*Operational case for the retention of internet connection records*" on 1st March 2016 which, as Mr Anderson described to the Joint Committee, indicated the ways in which police could find mass internet data useful. However, the Government is unable to demonstrate the necessity of the power.

In oral evidence to the Public Bill Committee on the Investigatory Powers Bill, on 24th March 2016, Mr Anderson said:

I last looked in detail at internet connection records almost a year ago now, and even an operational case had not been made. (…) I am afraid that I have not followed in the same technical detail as the Joint Committee on the Draft Investigatory Powers Bill and the Select Committee on Science and Technology the arguments on ***the extent to which they have been properly defined, the extent to which it will be feasible to produce these records or, indeed, how much it would cost.*** *Therefore, I cannot, I am afraid, raise any alarms on that or give you any reassurance, save to say that* ***these would appear to remain live issues****.*[29]

Liberty recommends that provisions for 'internet connection records' are removed from the Bill. In addition to having a devastating impact on freedom of expression and privacy online, the case for *necessity* of an ICR regime has not and cannot been made.

ICRs do not and cannot meet the stated policy aims

The value of ICRs in consistently and accurately identifying what internet communications services a suspect or suspected victim has used and when has been over-estimated and misunderstood. In an ICR Factsheet produced by the Home Office, it was claimed that ICR retention would identify what communications services a person has used and when, and thus "*allow the police to determine whether a missing person was using a particular*

[28] Joint Committee on the Draft Investigatory Powers Bill: Oral Evidence; David Anderson QC (QQ 61-75), p.19. http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf

[29] Public Bill Committee on the Investigatory Powers Bill: Oral Evidence, 24 March 2016, http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/160324/am/160324s01.htm

smartphone app or social media website prior to his or her disappearance".[30] In response, ISPA (Internet Service Providers Association) members *"pointed out the huge flaw in this argument*".[31] Often, ICRs would not accurately show *when* communications services have been used, and therefore would not be helpful for informing an accurate time frame for further communications data requests. This is because communications software (particularly on smartphones) makes frequent internet connections whether in use or not, remaining connected for a period of days, weeks or months.[32] Connection records show connection timestamps rather than access timestamps. ISPs and technologists have expressed serious concern that the Home Office has based an extensive, invasive data collection policy on misleading descriptions of what purposes ICRs could serve.

Even without using widely available privacy software, ICR data is "inexact and error-prone".[33] But the likelihood of bulk ICRs to prove vital in accurately identifying otherwise anonymous suspects of serious crime is vanishingly slim, as pointed out by ISPs and technologists.[34] Many online criminals do not, and certainly will not, offend using the internet under the conditions for which an internet connection record would need to be meaningful – that is, using a regular browser or public file sharing service on their own device, using personal internet connections, and without employing the most basic of the widely available anonymity tools to avoid detection. The use of privacy-enhancing and anonymising tools such as Virtual Private Networks (VPNs), which securely 'tunnel' internet connections; Tor, a secure browser that anonymises users' location and identity; and proxy web browsers that bypass filters and anonymise web browsing, is widespread and increasing exponentially. ICRs will be unusable and in fact misleading where such privacy tools have been used.

In addition, the retention of ICRs will push internet traffic, both legitimate and otherwise, into more protected spaces. This digital shift renders ICRs an invasive database of, almost exclusively, innocent citizen's digital lives, and forced retention of them a costly, out-dated, ineffective strategy.

---

[30] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[31] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html
[32] The main transmission protocol used online, TCP, can maintain a connection for hours, days, or even years; whilst protocols such as SCTP and MOSH aim to keep a connection active indefinitely, even with changes to IP addresses at each end or changes in connection.
[33] *Written evidence regarding draft Investigatory Powers Bill* - Tim Panton, 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25104.html
[34] *Written evidence regarding draft Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25065.html

ICRs can be dangerously misleading and falsely incriminating

The value of ICRs in consistently and accurately identifying access to illegal websites has also been over-estimated and misunderstood. The bulk retention of ICRs raises concerns about inaccurate and possibly incriminating representations of innocent individuals' internet use.

Each 'internet connection' involves the exchange of multiple packets of data. Some of these packets of data relate to the scripts, images and styles that constitute various elements of a webpage. An image or video embedded on a webpage may be hosted elsewhere and generates a separate 'internet connection', which may relate to a server (or 'site') the individual had no intention, or even knowledge, of accessing. Similarly, it is unlikely that ICRs will be able to distinguish between a webpage visited out of an individual's own volition and a pop-up. Therefore, an ICR could show repeated access to a website hosting indecent images, which could in fact represent an unwanted pop-up during innocent web browsing.

Bulk ICR retention could be exploited by hackers for nefarious purposes – for example, by embedding 'suspicious' scripts into webpages (e.g. linking to pornographic or jihadist websites), or spamming individuals with suspicious pop-ups.

In addition, many browsers and apps pre-cache links – that is, store data from linked webpages before they are even visited by the user, to improve access speed if it is selected. This also regularly creates involuntary, misleading internet connections. Clearly, bulk ICRs collected on a population-wide scale will lead to misleading, inaccurate and potentially suspicious information being generated on many innocent internet users.

ICRs have failed, at enormous public cost, where practiced before

In evaluating the efficacy of ICRs, we are informed by the case study of Denmark's Data Retention Law (*Logningsbekendtgørelsen*), effective 2007-2014, which required communication service providers to retain internet session logs.[35] **A self-evaluation report published by the Danish Ministry of Justice in December 2012 found that several years of collecting internet session data had not yielded any significant benefits for law enforcement - session data had played a minimal role in only one case.**[36] In fact,

[35] *Logningsbekendtgørelsen 2006* (https://www.retsinformation.dk/forms/r0710.aspx?id=2445). An English translation produced by the Ministry of Justice is available at https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf

[36] *Redegørelse om diverse spørgsmål vedrørende logningsreglerne* – Justitsministeriet, Dec 2012 (http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf). There is no English translation. The article "*In Denmark, Online Tracking of Citizens is an Unwieldy Failure*" - TechPresident, 22 May 2013, discusses the report (http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy).

Ministry staffers reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[37] In 2013, approximately 3,500 billion telecommunication records were retained in Denmark, averaging 620,000 records per citizen.[38] In June 2014, the Danish government repealed the obligation on operators to retain session data on the basis that it was "*questionable whether the rules on session logging can be considered suitable for achieving their purpose*".[39]

In response to widely expressed concerns about the UK adopting this failed model, the Home Office published a document comparing the Dutch case study with current UK plans.[40] Despite the rhetoric of "*important differences"*, there are only two minor differences in substance. Firstly, the UK Government promises (although will not make a statutory commitment) to meet communication service providers' costs *upfront* to cover the necessary infrastructural change, drain on resources, and generation and storage of data – whereas in Denmark, CSPs were remunerated *after* they implemented infrastructural change. It does not follow that this different mode of reimbursement will affect the usability of data, and if anything, gives rise to concerns about huge bills from internet companies to be footed by the taxpayer. Secondly, the Home Office makes much of the "*flexibility to tailor the design of ICR retention models*", referring to the lack of definition of ICRs and the intention to 'negotiate' with CSPs as to what data is generated and how. However, the Danish model also employed flexible regulation. The proclaimed difference is largely one of intent – the Home Office intends to achieve never-before-seen modes of tailored data collection at the population level through private 'negotiations' with CSPs. These proposals have proved unconvincing, unpopular, and alarming to CSPs.[41]

Threat to security posed by bulk retention of ICRs

The population's detailed internet connection records will be collected and stored by ISPs. This has generated significant concern among ISPs and the public alike, as this new trove of extremely valuable data will be attractive to criminal hackers and difficult to protect. When a similar plan to collect 'web logs' was proposed in 2012, the **Joint Committee on the Draft Communications Data Bill concluded that it would create a**

[37] Ibid.
[38] *Written evidence on Investigatory Powers Bill: Technology Issues* - IT-Political Association of Denmark, 2 Dec 2015, p.2
[39] *Justitsministeren ophæver reglerne om sessionslogning ("The Ministry of Justice repeals the rules about session logging*) – Justitsministeriet, 2 June 2014, http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning
[40] *Comparison of internet connection records in the Investigatory Powers Bill with Danish Internet Session Logging legislation* – Home Office, 1 March 2016
[41] See written and oral evidence to the Joint Committee and the Science and Technology Committee.

> **"*honeypot for casual hackers, blackmailers, criminals large and small from around the world and foreign states*".**[42]

In their final report, the Joint Committee noted that:

> *"storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn*".[43]

The Joint Committee on the draft Investigatory Powers Bill noted that "*data theft remains an ongoing challenge".*[44]

This wealth of data in the wrong hands could be used for identity theft, scamming, fraud, blackmail, and even burglaries, as connection records can show when internet access occurs in or out of the house, representing a daily routine. This is an unacceptable level of risk to inflict on innocent internet users. At a time when the UK is plagued by prolific hacks (e.g. TalkTalk, Vodafone, Vtech), taking the title as the most hacked country in Europe and the second most hacked in the world,[45] it is extraordinarily irresponsible to coerce private companies with the burden of generating, storing and protecting vast swathes of revealing data on the general public. Companies are unable to guarantee protection of the customer information they already have – burdening them with new data of unprecedented volume and value will have disastrous effects for the UK's internet industry and the safety of British internet users.

In addition to the obligation on UK telecommunications operators, the Bill places a duty on overseas operators to collect and retain ICRs on UK citizens.[46] This creates an extra set of concerns for UK citizens' privacy and the protection of extremely revealing data in other jurisdictions. The UK Government's general insistence on extraterritorial application of bulk communications data retention powers sets a "*disturbing precedent*" for other, more authoritarian countries to follow, as Mr Anderson pointed out in his independent review.[47]

---

[42] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.
[43] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, pp.28-29
[44] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Para. 174
[45] Internet Security Threat Report, 2015 – Symantec, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf. Reported on in, British companies bombarded with cyber attacks – Sophie Curtis, The Telegraph, 14 April 2015.
[46] Investigatory Powers Bill 2016, clause 86
[47] A Question of Trust: Report of the Investigatory Powers Review – David Anderson Q.C., June 2015, p.207

ICR retention will not be able to meet its stated purposes, and certainly not with any greater efficacy than the targeted surveillance methods available for investigations; in fact, it could easily cause false suspicion. Arguably, the £175+ million budgeted to fund telecommunications operators to spy on their customers would be better spent on frontline staff or community policing.

The Bill provides the Agencies with access to bulk ICRs

Lord Rosser asked the Government to clarify whether the intelligence agencies might seek to attain internet connection records in bulk, which is clearly provided for in the Bill. Lord Keen responded,

> "*it is of course worth being clear that current legislation would allow the agencies to acquire internet connection records in bulk*" .

Whilst law enforcement access to ICRs would be on a case by case targeted or thematic basis, with three broad routes to access described above, the Agencies' access to ICRs would be mass and indiscriminate. Lord Paddick described this as, "*a rather alarming prospect which I do not think has yet been raised in the public consciousness".*

Liberty shares the concerns of Labour, Liberal Democrats, the SNP and the Green Party about the nature of ICRs and the overly broad access to them by both police and the intelligence agencies. The ICR regime is a fundamentally excessive, unacceptably intrusive proposal that would threaten multiple rights, and as such, must be opposed.

We urge parliamentarians to reject the unnecessary power to generate and retain internet connection records.