OPEN RIGHTS GROUP - INTERNET CONNECTION RECORDS

Open Rights Group is the UK's only digital campaigning organisation, working to protect the rights to privacy and free speech online. With 3,200 active supporters, we are a grassroots organisation with local groups across the UK. We believe people have the right to control their technology, and oppose the use of technology to control people.

Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share and learn across the world. But for all the benefits, technological developments have created new threats to our human rights. We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions and technical projects.

In this submission we will focus on the proposals around internet connection records (ICRs)

1. **What are ICRs**

According to the Guide to Powers and Safeguards provided in the Investigatory Powers Bill (IPB), Internet Connection Records (ICRs) are one of the top three key new aspects in the draft legislation, together with the consolidation of legislation and the changes to authorisation and oversight. As such they should be subject to special scrutiny, and we would hope to have absolute clarity as to what exactly these ICRs are and how they will be used.
The Operational Case for the Retention of Internet Connection Records presents ICRs in very limited terms:

ICRs comprise a very narrow set of data, such as numerical internet protocol (IP) addresses and port numbers – which may be used to establish that a particular device accessed a particular internet service or website – as well as details of the time that a specific service was accessed.

Unfortunately, this concise definition is not reflected in the actual bill. The retention regime is much broader that stated, and it appears that ICRs could be used for a much broader range of purposes thanstated in the guidance.

2. Retention of ICRs

Below we present some specific issues with ICRs, but our starting point is that bulk retention of communications data is disproportionate. The EU Data Retention Directive was struck down and ICRs appear to be far more intrusive. We believe this power contravenes Article 8 of the European Convention on Human Rights and if challenged in court it would be found unlawful.

2.1 No proper definition of ICRs under an expanded data retention regime

ICRs are not properly defined in the part of the Bill that authorises data retention. Clause 71(9) of the Bill provides for the retention of “relevant communications data”:

communications data which may be used to identify, or assist in identifying, any of the following—
(a) the sender or recipient of a communication (whether or not a person),
(b) the time or duration of a communication,
(c) the type, method or pattern, or fact, of communication,
(d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted,
(e) the location of any such system, or
(f) the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program.

The documents provided by the Home Office repeatedly focus on the last item in the list, but ICRs could involve any of the above. The list goes further than the current Data Retention Regulations 2014[1]. For example, there is a new requirement relating to the pattern of communications, which could form the basis for attempting to unmask certain types of encrypted data.

The retention provisions in the draft bill do not define ICRs as a discrete type of data to be kept separately from any other relevant Internet communications data. The only definition in the draft bill of ICRs is to be found in clause 47 (6), in the part of the bill dealing with authorisations, not retention. Here an ICR is a type of *communications data* which

(a) may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and
(b) is 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).

ICRs are defined by their use and access regime, and could be understood very narrowly as a list of websites visited or services used, or quite broadly as covering almost all the types of communications data.

2.2 A new requirement to generate data

The requirement to **create** and retain this kind of data is completely new. The explanatory notes accompanying the Bill claim that an ICR is "captured by the company providing access to the internet", but this is not always the case. Telecommunications operators may have the theoretical ability but not the need, to generate these records. In some cases they may need to transform their systems and the Bill would force them to do so. The government estimates that this will cost

[1] http://www.legislation.gov.uk/uksi/2014/2042/schedule/made

£174.2 Million over 10 years, but there is not agreement among the technical community on whether this would cover all the associated costs.

2.3 Expanded scope of telecommunications operators

These retention provisions could involve a very broad range of data, particularly as the scope of the Bill goes beyond traditional providers. Clause 193 (10) defines "telecommunications operator" as a person who either offers or provides a telecommunications service to persons in the UK, or controls or provides a telecommunication system reaching the UK. A similarly expanded definition can be found in the DRIPA 2014, but the draft IPB goes further to cover private networks. Who is a *telecommunications operator* can be interpreted very broadly to go well beyond the Internet Service Providers used as an example in all the documentation provided by the Home Office. All kinds of access and connection logs could be demanded from many UK organisations. In some cases it may be difficult to establish who exactly is be the operator, such as in subcontracted or collective Internet provision in hospitals or schools.

3. Identification of devices under CTSA

Problems around the identification of communications equipment have been discussed on multiple occasions. They were central to the rejected Draft Communications Data Bill, and legislation on this matter was rushed in as part of the Counter-Terrorism and Security Act 2015 (CTSA). The Home Office did not consult at the time with industry, according to the Internet Service Providers Association (ISPA).[2] Less than a year later the Home Office claims that these provisions are not good enough and need to be replaced. This should raise concerns as to whether the measures being proposed in the current draft bill will actually deliver.

Section 21 of the CTSA[3] amends Section 2(1) of the Data Retention and Investigatory Powers Act[4] 2014 (DRIPA), and as with DRIPA these clauses would sunset at the end of 2016. The clauses introduce a new type of data that is to be retained, namely "relevant internet data". This is defined as communications data that relates to an internet access service or an internet communications service, which may be used to identify, or assist in identifying, the internet protocol address or other identifier which belongs to the sender or recipient of a communication. The definition of relevant internet data excluded specific types of data.[5] Our understanding is that these exclusions could cover data relating to website use and which programs are used as well as internet routing data.[6]

---

[2] http://www.ispreview.co.uk/index.php/2014/11/uk-counter-terrorism-security-bill-mean-isps.html

[3] http://www.legislation.gov.uk/ukpga/2015/6/part/3/enacted

[4] https://wiki.openrightsgroup.org/wiki/Data_Retention_and_Investigatory_Powers_Act_2014

[5] under subsections 3(c)(i) and (ii) of clause 17[4]

According to the Home Office, the main reason for those reforms was the widespread use of Carrier Grade NAT by internet providers, where a single Internet Protocol (IP) address - the unique identifier of a machine connected to the global internet - is shared by several devices. This is particularly common with mobile phones. The provisions in the CTSA were expected to allow the use of other data, such as MAC addresses associated with hardware and specific *"port numbers"* to be able to associate the use of an IP address at a particular time with an identified user in the real world.[7]

Unfortunately, according to the Home Office's operational case for ICRs, the provisions in the CTSA 2015 were not enough to identify some internet users:

"where someone is using an internet service from an overseas company, such as an email website, IP resolution will rely on that company happening to hold enough data to match additional data that is retained by the UK internet access provider under the Counter Terrorism and Security Act. Such information will regularly not be provided."[8]

In the same operational case document quoted above the Home Office stated that the CTSA *"reflected the extent of cross-Government agreement in the last Parliament"*. The Home Office should be asked by Parliament why they rushed in legislation with the apparent knowledge that it would not deliver what was expected.

We believe that more transparency is required as to the expected outcomes. It is difficult to estimate the claims of the Home Office that ICRs will solve the problems that CTSA did not solve, or whether in a few months we will see demands for more legislation.

4. Access to ICRs

The documents supporting the draft bill stress that there would be strict limits on access to ICRs

"Applications to acquire ICRs can only be approved using the stringent application process for communications data requests (…) and only for a limited set of statutory purposes and subject to strict controls. Local authorities will be prohibited from acquiring ICRs."[9]

We see several problems with the access regime proposed for ICRs:

---

6 https://www.openrightsgroup.org/ourwork/reports/briefing-on-counter-terrorism-and-security-bill

7 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388035/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf

8 LINK OPERATIONAL CASE

9 Guide to powers and safeguards p. 26

4.1 Lack of judicial authorisation

ICRs will be accessed under the general regime for communications data, which means that there would be no judicial authorisation or "double lock" for accessing internet connection records. The oversight body proposed in the draft bill would carry out audits and possibly inspect a fraction of the warrants issued. ORG has called for full judicial authorisation, which is the process in many other democracies.

4.2 Unclear restrictions on identification purposes

The Home Office has made the case that access to ICRs would be governed by a narrow set of objectives around the identification of devices or services by police and other authorised bodies.

Clause 47 (4) of the draft bill restricts the purposes for obtaining ICRs (or derived data), which the explanatory notes describe as:

a. To identify the sender of an online communication; this will often be in the form of IP address resolution and the internet service used must be known in advance of the application.
b. Identifying which communication services a person has been using, for example determining whether they are communicating through apps on their phone.
c. Identifying where a person has accessed illegal content, for example an internet service hosting child abuse imagery.[10]

The first purpose of identifying the sender of a communication is fundamentally different from identifying everything a user does online. These should be treated as completely separate purposes.

The third purpose around identifying access to illegal content would seem a corollary to the recording of all online activities, and it is unclear why it requires to be listed separately. The Home Office should clarify whether they understand this to imply an extra monitoring obligation for operators.

More broadly, we do not find that the above access provisions fundamentally restrict what can be done with new types of Internet data that could be retained under the broader provisions in the bill.

As we saw in above, ICRs are not defined as a separate category in data retention, only by how they may be used to identify services being accessed by users. The above provisions would appear to be a circular construct where data that may identify what a user does online can only be used for that purpose. Additional safeguards would be needed. We are concerned that without a definition of ICRs in retention the same data might be accessed for other purposes.

It is also very unclear what restrictions exist in the draft bill for any further uses of internet data retained under the broad provisions in section 71. The current regime

[10] explanatory notes § 120, p. 21

already allows for access to Internet related data without the above restrictions, and it appears that this would continue, albeit with a bifurcated regime for some data labelled ICRs.

4.3 Pre-acquisition analytics and data mining through the request filter

One of the most concerning aspects of the draft bill is the "request filter", already proposed as part of the rejected Communications Data Bill. The *filter* would allow the police and authorised public bodies to search and analyse retained communications data.

This "filter" is described in the impact assessment as a *safeguard* because it would potentially reduce the amount of data that would be forwarded to the police, but we find the filter actually increases the privacy intrusiveness of the bill. By conducting intrusive data mining across a range of databases held by service providers, the "filter" violates the privacy of an unlimited number of innocent people.

The intrusiveness of storing details of all online activities of the population grows exponentially with the "filter". For example, police would be able to easily identify all participants at multiple political demonstrations broadcasting critical videos from their mobile phones.

4.4 Bulk acquisition

The use cases presented to justify retaining ICRs are based on police work and individual access, but the records would be subject to the bulk acquisition powers outlined in Part 6 of the draft Bill. This would allow the Security and Intelligence Agencies to go beyond those narrow purposes to perform sophisticated analytics able to generate new leads on potentially suspicious behavioural patterns, and ultimately map the internet usage of the whole UK population.

The current secret regime for the acquisition of bulk communications data under the Telecommunications Act 1984 has only been avowed with the publication of the draft bill. We do not believe that acknowledging the existence of these provisions for bulk access will ever make them proportionate under human rights requirements, and this whole part of the bill should be scrapped.

The arrangements for the implementation of the current regime published with the bill[11] exclude ICRs, but there is nothing in the draft bill carrying through these restrictions after the Telecommunications Act is superseded by the IPB. As with the filter, the intrusiveness of the general provision would be amplified by collecting online histories.

[11] Arrangements For The Acquisition Of Bulk Communications Data Pursuant To Directions Under Section 94 Of The Telecommunications Act 1984

The government created an access regime for communications records, with special authorisations and procedures sanctioned by Parliament under RIPA. We now learn that successive Secretaries of State bypassed Parliament, abusing legal loopholes to create a secret bulk access mechanism that did not contain any of the safeguards provided by law. We remain concerned that there are no guarantees that this behaviour may not happen again.

5. The case for ICRs

From the available documents presented with the draft Bill we are concerned that ICRs are presented as a solution to problems that could be solved by other less intrusive means.

The Report of the Investigatory Powers review by David Anderson asked for a "compelling operational case" for the retention of third party data, such as ICRs. The Home Office has provided such a document with the draft bill. We find it does not fully support the proposed measures, but instead points at alternative, more targeted, approaches that would not require mass surveillance.

5.1 ICRs and serious crime

As highlighted by researcher Nora Ni Loideain,[12] the "Operational Case for the Retention of Internet Connection Records"[13] supplied with the draft Bill is supported by only two studies: one on referrals made by the National Centre for Missing and Exploited Children (NCMEC) and another one on the use of mobile devices in serious crime investigations. Both relate to serious crime, but there is no evidence justifying allowing access to IPRs for the many other purposes under the IP Bill.[14] These include preventing disorder, protecting public health and financial stability. The draft bill would give 46 public authorities (including the Food Safety Authority) access to all types of communications data, including IPRs.[15]

5.2 ICRs as substitute for interception warrants

One of the stated purposes of the ICRs is to determine how a known device has accessed communications services and illegal websites. The *Operational Case* makes clear that security services have access to this kind of information in relation to suspects in criminal investigations through the use of targeted intercept warrants.

---

12 https://opendemocracy.net/digitaliberties/nora-ni-loideain/uk-investigatory-powers-bill-one-step-forward-two-steps-back

13 LINK OPERATIONAL CASE

14 IP Bill, s.46(7)

15 IP Bill, Schedule 4

The argument is made that these warrants can only be used for narrower purposes than communications data (serious crime, national security and economic well-being of the nation) and therefore are not available in cases such as missing persons investigations.

The argument presented by the Home Office is that the majority of investigations considered suitable for acquiring ICRs are not "serious" enough to qualify for the current interception regime. This would be moving the bar considerably in the opposite direction by allowing access to the communication history of a much broader range of people, in addition to requiring everyone's data to be recorded..

The committee needs to query what are the reasons for the Home Office to dismiss the opportunity of obtaining device information in a targeted manner without the need to resort to mass surveillance. It would appear that the unjustified drive to leave interception of communications out of the criminal justice system, as the exclusive remit of a small set of security agencies under direct control of ministers, is creating an unnecessary problem.

The draft legislation is a missed opportunity to reform interception. Instead the Home Office is proposing a solution to the problem of accessing information about a small number of suspects that involves intruding in the privacy of the vast majority of innocent internet users.

If targeted interception of known suspects can work, surely the preferred solution here would be to make interception available for a wider but specified range of purposes - including missing children - under judicial authorisation, and admissible in court - as is the case in most democratic countries.

5.3 Weak arguments for broad data retention

The examples used the Impact Assessment for Communications Data[16] to support ICRs in some cases involve ongoing investigations into known suspects that could be dealt with through targeted data preservation, instead of keeping the internet history of the entire population.

The case for IP resolution is stronger than the arguments about knowing the apps used by suspects. In one example, the police made use of an undercover officer to obtain this kind of information (page 13). This would appears to be the correct procedure: targeted police work instead of mass surveillance of every internet user.

The *Operational Case* includes the example of an "investigation into the distribution of indecent imagery of children where CD (communications data) could not identify how members of a criminal network were communicating and only thanks to the seizure of devices was it possible to identify more than 250 additional suspects".

[16] IPB Impact Assessment Communications Data (available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473773/Impact_Assessment-Communications_Data.pdf)

Again it would appear that seizing equipment, another established investigative procedure, has yielded results.

In other examples used it is unclear what exact problems the police have with the current provisions in the CTSA for IP resolution that require expanding the concept of ICRs. The perspective that transpires throughout the documents is that it would be easier to be able to simply query the retained data instead of following more cumbersome processes. The police should be efficient and effective and not suffer form excessive burdens. But the operational case does not discuss the relative proportionality of different forms of intrusion, just how technology could help minimise police efforts, and a more balanced analysis is needed. Technology opens up possibilities for what can be done, but this does not mean it should be done.

6. Other concerns

6.1 Are ICRs internet histories?

The argument has been made that internet records would only link a user or device with the internet identifier for a whole website or service, but not the individual page, and that therefore this is less intrusive and not equivalent to an internet history. For example, the record would show that user X has visited www.google.com, but would not give details of the searches performed, as these would be classed as content, not communications data.

The first problem with this argument is that cumulative information of websites visited can give a good picture of someone's lifestyle. Single visits to some sites can be sensitive even if we only know, for example, that someone visited an abortion clinic's site but not the specific sections.

Journalist Mikey Smith has published an example of the different between a full web page address and websites:

https://twitter.com/mikeysmith/status/661906655093747712

The second and much more concerning issue is that comprehensiveness of the proposed measures goes beyond individual web histories. If this draft bill goes ahead, there would be a distributed database of every website visited and mobile app used by every person in the country. The ability to process this pool of data in order to build an understanding of sustained patterns of behaviour at the population level is highly intrusive. Here the bulk acquisition powers of the Security and Intelligence Agencies are of particular concern, although the filtering requirements could also be used by police to perform sophisticated population analytics.

Finally, we consider that the proposals do not sufficiently consider the security risks of generating and storing this kind of information. We have seen many data breaches in recent times. The attacks on ISP TalkTalk showed that poor security is widespread even among major companies[17]. The recent attack on the US Office for Personnel Management demonstrate that even high security government institutions holding data on vetted staff are not safe[18]. The hacking of the contacts website Ashley Madison shows that the leaking of very sensitive data can lead to very serious consequences, including possible suicides[19]. The case of Vodafone Germany points at the risk of insider attacks[20]. Despite clauses in the bill requiring security measures, nobody can promise the data will be 100% safe. The best security is to limit data to what is strictly necessary.

6.2 What exactly will be an ICR?

[17] http://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack
[18] http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0
[19] http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html
[20] http://www.securityweek.com/attacker-steals-data-2-million-vodafone-germany-customers

Despite the various documents and explanations accompanying the draft bill, there is a lack of clarity as to what exactly will constitute an ICR. Operators would be forced to record logs of access to online services, but there could be huge differences on how this is interpreted and the impact of the measures.

The assumption behind the case for ICRs appears to be that there is a simple two way interaction between a user and a remote service or website. For example, a user would type the name of a website and read it, but the operations behind this simple interaction can be quite complex.

Internet services providers asked to keep a log of all the websites visited by a user would be faced with many issues to be able to correctly link one of their customers with a remote server.

Here we highlight several potential issues to consider in order to know what exactly may be recorded. This is not a comprehensive list nor a detailed technical analysis of the options for internet providers to comply with the requirements to record detailed internet usage.

Redirection

Many web requests will involve multiple redirects, and the nature of these means the location from which the action is performed or other information about it may well be implied. It is unclear whether the ICR should capture the original requested website, the final destination, the redirects or all these.

Link pre-fetching

Modern web browsers provide an advanced feature that uses *"idle time to download or prefetch (sic) documents that the user might visit in the near future. A web page provides a set of prefetching hints to the browser, and after the browser is finished loading the page, it begins silently prefetching specified documents and stores them in its cache. When the user visits one of the prefetched documents, it can be served up quickly out of the browser's cache."*[21]

This means that the ISP would keep a record of a visit to websites that the user had never actually seen or clicked through. There could be measures to filter out this kind of traffic but these would involve even more detailed and intrusive traffic analysis.

Proliferation of advertising and tracking

The growth of software to block third party adverts has provided a realisation that large amounts of internet traffic nowadays is related to advertising and tracking. When a web page is opened in a browser it generates multiple connections to companies that will try to provide personalised advertising. Advertising companies

[21] https://developer.mozilla.org/en-US/docs/Web/HTTP/Link_prefetching_FAQ

place small files in the user computer that allow the tracking of visitors across multiple websites and also generate their own traffic.

Images and videos - even fonts - are increasingly linked from third party specialist services, which will also trigger an external connection from the user device. In principle those multiple connections could be recorded as visits to those internet addresses. While there may be ways for an ISP to filter such traffic out it may not be easy.

In some cases there will be links where the user is not even using the service at all. Facebook has been ordered by the Belgian privacy authority to stop tracking internet users who are not even members of Facebook[22]. There are viruses that will make the infected computer trigger fake visits to websites in order to generate bogus advertising revenue, and could even include links to illegal content

6.2.3 The need for intrusive internet traffic analysis

We believe that the proposed ICRs will by necessity require performing very intrusive and sophisticated analysis of internet traffic.

Internet technologist Tim Panton[23] has published an analysis of what kind of information may be collected by operators as part of ICRs. He recorded the internet traffic of his home connection and found some problems. The data recorded was not able to deliver the requirements in the bill for data that would allow the identification of a visitor to a site. Panton also found that the recording of this data would tell which were the main websites he used, but not exactly how he used them, and that the data missed some messaging applications, including Skype.

In order to dig deeper into users activities, including the use of messenger applications such as Skype, ISPs would need to perform detailed analysis of the traffic, looking into individual internet packets and reconstructing internet sessions. A session involves an exchange of communications between two computers. For example, a visit to a website, a message, all involve sessions, composed of many packets, also called “events”.

Adrian Kennard,[24] CEO of ISP Arnold and Andrews, performed some tests and found that a computer simply logging on to Facebook and clicking a like button triggered hundreds of single events. He has described some of the technical difficulties involved in logging such sessions, as many internet communications do not operate in a way that can be recorded as independent events.

The requirement for ICRs will involve detailed analysis of communications, which is highly intrusive and more akin to interception than data acquisition.[25]

---

22 http://www.bbc.co.uk/news/technology-34765937

23 https://babyis60.wordpress.com/2015/11/13/the-investigation-of-packets/

24 http://www.revk.uk/2015/11/what-is-internet-connection-record.html

25 http://www.projectpact.eu/privacy-security-research-paper-series/%231_Privacy_and_Security_Research_Paper_Series.pdf

6.2.4 The need to record full web addresses

The creation of ICRs of web interactions could require the recording of full URLs - the text in the so-called address bar at the top of a web browser that identifies the web page being displayed. These would then be edited in order to generate a history of sites visited, which is not as simple as it seems.

Many websites nowadays are not just texts with images but sophisticated software programmes pulling data and ancillary functions from a variety of online sources. Some modern web technologies, such as REST, generate URLs that often include as parameters the data necessary to perform these programmatic functions. A record of what specific “service” was accessed may well require more than just the top level name of the website (e.g. google.com)

Further, the use of proxy servers, load balancers and Content Delivery Networks such as Akamai mean that the target URL is often embedded in the URL of an intermediary, so that recording the true destination requires semantic understanding of the URL and analysis post-capture.

All that points to the probability that for operational reasons the full URL and not just the domain name will be captured and stored and then "filtered". This activity should be classed as interception.

These examples show some of the issues raised by what appears to be a simple request to identify who has visited a site or what websites a user has visited.

The above examples only refer to traffic by Internet Providers. Once data retention provisions are extended to other internet companies such as providers of Virtual Private Networks it will be increasingly difficult to precisely define what may be an ICR.

The Committee may wish to ask for clarification as to what exact information would be necessary to deliver the stated objectives of the draft bill, and possibly obtain some examples of model retention notices that could be imposed on various types of telecommunications operators.

6.2.4 GCHQ and ICRs

In addition to the confusion about what traffic would have to be recorded and stored, we are also concerned about the possibilities that recording all internet traffic creates for intrusive monitoring beyond individual histories. In principle the draft bill would give the intelligence and security services the powers to acquire any bulk dataset in the country, including the data from advertising companies that track internet users across the web.

Leaked documents from GCHQ show that the agency has an array of systems designed to provide specialists insights on various aspects of the activities of

millions of Internet users, such as website history, location and maps of social relationships.[26]

The agency uses all kinds of data picked from the Internet for these purposes:

"environmental information and various forms of 'Internet Pocket Litter' (e.g. cookies, delete keys). These new capabilities and forms of data have the potential to become our most highly valued and prized data.[27]

These small pieces of Internet traffic are called by the agency TDIs – Target Detection Identifier – and are extremely intrusive because they provide the "who, when, where". They "are definite indicators of presence that are unique and persistent for a user/machine." These TDIs can be associated to many other bits of information, such as emails from airlines or Yahoo! webcam images. For the agency they are the "fundamental atom of the Internet age,"[28] and they store them for up to six months.[29]

One of GCHQ's programmes called KARMA POLICE aims to correlate every user visible in bulk data with every website they visit, hence providing either (a) a web browsing profile for every visible user on the Internet, or (b) a user profile for every visible website on the Internet. It builds correlations, bulk unselected identifiers (TDIs), and websites by comparing information about which identifiers have been seen at approximately the same time, and from the same computer, as visits to websites.

GCHQ have been undertaking large scale interception activities that mirror aspects of what is being proposed for ICRs. No mention is made of this in any of the supporting documents. No case is made for the need of ICRs with reference to GCHQ's existing bulk interception capability. Any analysis of the need to create a national linked database of internet connection records must be undertaken in the context of these revelations.

Conclusion

ORG believes that the measures to introduce ICRs are problematic and should be removed from the legislation.

In summary:

- bulk retention of online activities is disproportionate and unlawful
- the proposal lacks clarity and is far more intrusive than Home Office statements would suggest

---

26 hhttps://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities

27 http://theintercept.com/document/2015/09/25/access-vision-2013/

28 http://theintercept.com/document/2015/09/25/tdi-introduction/

29 http://theintercept.com/document/2015/09/25/data-stored-black-hole/

- purpose restrictions do not provide sufficient safeguards
- the technical implications of ICRs, are not understood, because ICRs are not defined, and there is not enough technical information to make a more detailed appraisal
- the creation of ICRs may involve activities that should be classed as interception rather than acquisition of data
- the lack of reference to GCHQ's activities, makes even more difficult to consider the claimed benefits.
- there appear to be more targeted alternatives to find out services accessed by individuals
- measures to provide the identification of the starting point of a communication may be improved without requiring the detailed recording of the internet activities of the whole population
- the security risks are too great

David Anderson did not just ask for an operational case for ICRs. His full recommendation was:

"There should be no question of progressing proposals for the compulsory retention of third party data before such time as a compelling operational case may have been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions is currently satisfied."

We believe that his analysis applies to the draft bill.