LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on Parts 3 and 4 of the Investigatory Powers Bill for Committee Stage in the House of Commons

April 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

Introduction

Liberty welcomes the opportunity to provide briefing and amendments in relation to Parts 3 and 4 of the Investigatory Powers Bill.

This briefing sets out the following proposals for reform to Part 3:

- Introduce a system of judicial authorisation for access to communications data, replacing the proposed system of internal authorisations to relevant public authorities and notices to telecommunications providers
- Limit the purposes for which communications data may be accessed to national security, the prevention or detection of serious crime, and to protect life.
- Insert a threshold of reasonable suspicion that a serious offence has or is likely to take place when a warrant is sought to prevent or detect serious crime.
- Limit the definition of "relevant authority" for the purposes of who can access communications data to police forces and the security services, except in order to protect life
- Prevent modification of "relevant authorities" definition by the Secretary of State
- Remove provision to establish a filter
- Add whistle-blower protection
- Provide for enhanced protection for confidential and privileged communications

This briefing sets out the following proposals to amend part 4:

- Establish a system of prior judicial authorisation for data retention warrants, to be issued on application by a relevant public authority. This would replace the current system of data retention notices issued by the Secretary of State.
- Provide for warrants to be available for the purposes of national security, preventing and detecting serious crime, and to protect life.
- Ensure a targeted retention scheme by requiring a warrant to name or otherwise identify a person, organisation, premises or location to which it relates
- Delete provisions relating to Internet Connection Records.

Intrusive nature of modern communications data

Communications data provides a detailed and revealing picture of somebody's life in the digital age. As defined under DRIPA and RIPA it can disclose the date, time, duration and type of communication, the type of communication equipment used, its location, the calling telephone number and the receiving telephone number. This can reveal personal and

sensitive information about an individual's relationships, habits, preferences, political views, medical concerns and the streets they walk. As the CJEU has put it:

> *"those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*[1]

In December 2013, US District of Colombia Judge Richard J Leon found that a lawsuit challenging the NSA's previous regime of bulk metadata collection demonstrated a "substantial likelihood of success"[2] and said of modern data metadata:

> *"I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval…Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment."*

Indeed in many circumstances the picture of someone's life that can be created through examination of communications data will be more revealing than the content of many of their communications. As Stewart Baker, former senior counsel to the US NSA observed in 2013, metadata *"absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."*[3] The value of metadata and the use that the UK's closest ally is prepared to make of it was left beyond doubt following comments by the former head of the NSA, Michael Hayden in 2014: "*We kill people based on metadata*."[4] Furthermore, there are many situations in which just the fact of a single communication and the identities of the parties speaks volumes: the phone call from a senior civil servant to a reporter on a national newspaper immediately before a major whistle-blower scandal fills the

---

[1] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).

[2] Klayman v Obama in the United States District Court for the District of Colombia, 16 December 2013, available at: http://apps.washingtonpost.com/g/page/world/federal-judgerules-nsa-program-is-likely-unconstitutional/668/.

[3] Stewart Baker, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-killpeople-based-metadata/

[4] General Michael Hayden, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-killpeople-based-metadata/

front pages; the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody.

The Government seeks to diminish the importance and sensitivity of communications data by distinguishing it from the content of communications. At one time a firm distinction between communications data and content would have been more credible, for example when communication was primarily by letter: everything inside the envelope is content, everything on the outside communications data. However, this distinction has been eroded by the scale of modern internet and mobile phone usage. As communications have become increasingly digital, the data generated is much more revealing and copious than before, allowing the state to put together a complete and rich picture of what a person does, thinks, with whom, when and where. Often, communications data can be of more use than content: it is expansive, easy to handle, analyse and filter; and, it tends to be collected in a consistent manner. In 2015 the ISC remarked: *"**We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications."***[5]

Incompatible with court judgments

Liberty fully supports a targeted and proportionate data retention and access system, and understands its value to law enforcement. However we believe that the current retention and access regimes – not to mention the proposal to impose further obligations on ISPs to generate and retain ICR data in the Bill - violate human rights law and will be found in breach of the European Charter of Fundamental Rights and Freedoms, when the CJEU considers communications data retention and acquisition once again in 2016. In April 2014, the CJEU ruled in Digital Rights Ireland that the EU Data Retention Directive which mandated blanket data retention for between 6 -24 months was invalid due to its sweeping interference with privacy rights. The CJEU acknowledged the important role of data retention and access for the prevention and detection of serious crime but laid out the following ten principles to ensure compliance with human rights standards –

- restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);

[5] *Privacy and Security: a modern and transparent legal framework* - Intelligence and Security Committee, March 2015, paragraph 80.

- provide exceptions for persons whose communications are subject to an obligation of professional secrecy (paragraph 58);
- distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
- ensure retention periods are limited to that which is ‘strictly necessary' (paragraph 64);
- empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);
- restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);
- limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);
- ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access (paragraph 66);
- ensure destruction of the data when it is no longer required (paragraph 67); and
- ensure the data is kept within the EU (paragraph 68).

Three months after the judgment, the UK Government responded with emergency legislation – the Data Retention and Investigatory Powers Act 2014 (DRIPA) - which was rushed onto the statute book in 7 days in July 2014. Prior to the decision in Digital Rights Ireland, senior courts across Europe had annulled domestic legislation seeking to implement the EU Directive – including Bulgaria, Romania, Germany, Cyprus and the Czech Republic. Following the judgment, courts in a further six Member States, including five courts of final appeal, have relied on DRI in holding national data retention legislation invalid – including courts in Austria, Slovenia, Belgium, Romania, Netherlands, Slovakia.

Liberty is currently representing David Davis MP and Tom Watson MP in their legal challenge to DRIPA. In July 2015 the High Court upheld their challenge and struck down sections 1 & 2 DRIPA, finding them incompatible with the British public’s right to respect for private life and communications and to protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The High Court has found sections 1 and 2 of DRIPA unlawful on the basis that: they fail to provide clear and precise rules to ensure data is only accessed for the purpose of preventing and detecting serious offences, or for conducting criminal prosecutions relating to such offences; and: access to data is not authorised by a court or independent body, whose decision could limit access to and use of the data to what

is strictly necessary. The ruling observes that: *"The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome."*

The Government appealed the judgment to the Court of Appeal. In November 2015 the Court of Appeal referred two questions to the CJEU, namely (1) Did the CJEU in Digital Rights Ireland intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply? And (2) Did the CJEU in Digital Rights Ireland intend to expand the effect of Articles 7 and/or 8 of the Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR? On 4 May 2015, another CJEU reference on data retention post DRI was made by a higher court in Sweden asking whether a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime is compatible with EU law taking into account the Charter.

The outcome of these references will have significant bearing on the lawfulness of Parts 3 and 4 of the Bill. While Liberty strongly encourages Members of Parliament to delay consideration of these parts of the Bill until the judgment has been delivered, the following amendments seek to provide for a targeted, judicially authorised and human rights compliant regime in accordance with court judgments.

PART 3: ACCESS TO COMMUNICATIONS DATA

Judicial warrants for access to communications data

Amendment

Clause 53, page 42, line 13, after ‘power’ insert ‘of judicial commissioner’

Clause 53, page 42, line 13, delete ‘authorisation’ and insert ‘communications data access warrants’

Clause 53, page 42, line 14, delete sub-clause (1) and insert –

(1) A Judicial Commissioner may grant a communications data access warrant where the judicial commissioner considers -

(a) that it is necessary to obtain the data for the purposes of a specific investigation or a specific operation, and

(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved.

(2) The grant of a warrant is subject to restrictions set out in the rest of this Part.

Clause 53, page 42, line 26, replace ’designated senior officer’ with ‘warrant’

Clause 53, page 42, line 32, delete sub-clause (3)

Clause 53, page 43, line 4 delete ‘authorisation’ and insert ‘warrant’

Clause 53, page 43, line 14, delete ‘authorisation’ and insert ‘warrant’

Clause 53, page 43, line 16, delete ‘authorisation’ and insert ‘warrant’

Clause 53, page 43, line 25, delete ‘authorisation’ and insert ‘warrant’

Clause 54, page 44, line 19, delete ‘authorisations’ and insert ‘warrants’

Clause 54, page 44, line 20, delete sub-clauses (1), (2) and (3)

Clause 55, page 45, line 14, delete ‘authorisations and authorised notices’ and insert ‘warrants’.

Clause 55, page 45, line 15, delete sub-clause (a)

Clause 55, page 45, line 37, delete sub-clause (4)

Clause 72, page 57, line 28, delete ‘an authorisation or required to undertake by virtue of a notice given in pursuance of an authorisation,’ and insert ‘a warrant’

Clause 72, page 57, line 30, delete ‘the authorisation or notice’ and insert ‘warrant’

Effect

These amendments provide that in order to access communications data, a relevant public authority must seek a warrant from a Judicial Commissioner rather than undertake a system of internal authorisation.

Amendment

Clause 53, page 43, line 5, delete sub-clause (d)

Clause 53, page 42, line 26, delete 'the designated senior officer may authorise any officer of the authority to' and insert 'A warrant granted by a judicial commissioner may authorise the applicant or a telecommunications operator to'

Clause 55, page 45, line 14, delete 'authorisations and authorised notices' and insert 'warrants'

Clause 55, page 45, line 14, delete 'authorisations and authorised notices' and insert 'warrants'.

Clause 55, page 45, line 15, delete 'authorisation' and insert 'warrant'

Clause 55, page 45, line 24, delete sub-clause (2)

Clause 55, page 45, line 29, delete line 31

Clause 57, page 46, line 18, delete 'authorisations' and insert 'warrants'

Clause 57, page 46, line 20, delete 'authorisation' and insert 'warrant'

Clause 57, page 46, line 24, delete 'authorisation' and insert 'warrant'

Effect

These amendments provide for warrants to authorise conduct of a relevant public authority and require steps be taken by a telecommunications operator, removing the need for separate 'authorisations' to public authorities and 'authorisation notices' to telecommunications operators.

Amendment

Clause 53, page 42, insert new sub-clause (1A) –

(1A) The Judicial Commissioner may grant a warrant on application from:

(a) An officer from a relevant public authority involved in the relevant investigation; or,

(b) An individual designated by the relevant public authority to make applications for warrants to the Judicial Commissioner.

Effect

This amendment permits public authorities to determine whether applications for warrants are made directly from officers involved in an investigation or whether they wish to establish an internal process for doing so.

Amendment

Clause 53, page 42, line 25, insert new sub-clause (1B) –

(1B) A warrant must:

(a) name or otherwise identify the person or persons, organisation, premises, or location to which the warrant relates; and
(b) describe the investigation or operation to which the warrant relates.

Effect

This amendment specifies that warrants must state the investigation or operation to which they relate, as well as requiring warrants to name or otherwise identify the person, persons, organisation, premises or location to which the warrant relates.

Briefing

Communications data is currently retained by telecommunications operators for business purposes and in addition where they are required to do so under a data retention notice issued by the Secretary of State. Currently, access to communications data by law enforcement agencies and an array of other public bodies is predominantly self-authorising and requires no prior external oversight. Authorisation is by a designated person within the organisation seeking the access to surveillance under the "SPOC" system. This regime is replicated by the provisions in the Bill.

As outlined above, case law is clear that access to communications data can only be via a truly independent administrative or judicial body, and the current provisions do not provide for this.

It is entirely unacceptable for public authorities to be able to self-authorise access to revealing personal data. We do not seek to impugn the integrity of public officials or senior employees of our law enforcement agencies, but rather point out the reality that their primary concern will relate to the operational capacity of their agency. This is a matter of organisational culture and is perfectly understandable, but it is also a reality which mitigates in favour of independent third party authorisation. Decisions concerning necessity and proportionality can only be properly made by someone without any conflict, or perceived conflict, of interest. It is highly unlikely that the destructive surveillance activities of Metropolitan police CHIS would have continued under a system of prior judicial authorisation. This badly regulated practice, based on a system of internal authorisation, has led to collapsed prosecutions and convictions overturned. It has also led to gross human rights violations and untold harm. These scandals demonstrate the fatal problems of internal authorisation as currently permitted for number of RIPA surveillance techniques.

Towards the end of 2015, it was revealed that due to what a judge labelled “systemic” internal failings in the way the National Crime Agency applied for warrants, a number of trials were at risk of collapse.[6] Earlier in the year, Mr Justice Hickinbottom lamented an “egregious disregard for constitutional safeguards” within the NCA.[7] It seems clear that the risks of leaving vital safeguards solely in the hands of law enforcement agencies can offer no guarantee that proper procedures will be followed.

.

[6] See, for example, http://www.buzzfeed.com/tomwarren/the-national-crime-agency-is-in-chaos-over-unlawful-raids#.vfo4nk41Lv

[7] Chatwani & Ors, R (on the application of) v The National Crime Agency & Anor [2015 EWHC] 1283 (Admin)

Purposes for granting access

Amendment

Clause 53, page 43, line 39, delete ‘or of preventing disorder’

Clause 53, page 43, line 39, after ‘detecting’ insert ‘serious’

Clause 53, page 43, line 40, insert ‘where there is reasonable suspicion that a serious criminal offence has been or is likely to be committed, which includes to assist in investigations into alleged miscarriages of justice’

Clause 53, page 43, line 41, delete sub-clauses (c)-(f) and (j)

Effect

This would limit the ground for which a warrant may be granted to the interests of national security and preventing or detecting crime. These are the grounds for which interception warrants may be issued. In addition, this amendment would leave in place a ground of preventing death or injury.

Amendment

Clause 53, page 44, line 1, delete “or any damage to a person’s physical or mental health , or of mitigating any injury or damage to a person’s physical or mental health”

Effect

This is intended as a probing amendment to seek clarification as to the breadth and scope of the latter part of this ground. It appears that much of the language duplicates the description at the start of the clause ‘for the purpose of preventing death or injury’. It is also unclear what ‘mitigating injury or damage’ is intended to cover.

Amendment

Clause 53, page 43, line 41, insert ‘where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed’

Effect

This amendment would require that the ground of investigation of preventing or detecting a crime is tied to a reasonable suspicion that a crime has taken place.

Amendment

Clause 53, page 42, line 21, delete sub-clause (ii)

Effect

This amendment would delete the purpose of testing, maintaining or developing equipment, systems or other capabilities as a purpose for which a warrant may be approved.

Briefing

As drafted, the Bill would allow access to communications data for ten broad purposes. Case law, most recently Davis and Watson in the High Court, required legislation to restrict access to situations where is necessary and proportionate to prevent and detect serious crime. Similarly, elsewhere in the Bill targeted interception and other powers are restricted to use where is it necessary and proportionate for the purposes of national security and the prevention of crime. Given the intrusive nature of communications data, it is unclear why the Government has not chosen to restrict access to communications data to these same purposes.

To reflect the way in which communications data is used in situations such as missing person inquiries, the amendment leaves in place a purpose permitting access in situations where data is requested to prevent death or injury. However, the formulation as drafted is broad and unclear. We suggest that politicians probe the Government on the need for such a broad purpose.

Definition of relevant public authorities

Amendment

Clause 61, page 49, line 32, delete sub-clause (2) and insert -

(1) For the purposes of this Part, a relevant public authority is:
    (a) A police force maintained under section 2 of the Police Act 1996
    (b) Metropolitan police force
    (c) City of London police force
    (d) Police Service of Scotland
    (e) Police Service of Northern Ireland
    (f) British Transport Police Force
    (g) Ministry of Defence Police
    (h) Royal Navy Police
    (i) Royal Military Police
    (j) Royal Air Force Police
    (k) Security Service
    (l) Secret Intelligence Service
    (m) GCHQ
    (n) National Crime Agency

(2) Where a warrant is issued for the purpose in 53(7)(g), a relevant public authority also includes:

    (a) A National Health Service Trust established under section 5 of the National Health Service and Community Care Act 1990 whose functions include the provision of emergency ambulance service
    (b) A fire and rescue authority under the Fire and Rescue Services Act 2004
    (c) Northern Ireland Ambulance Service Health and Social Care trust
    (d) Northern Ireland Fire and Rescue Service Board
    (e) Scottish Ambulance Service Board
    (f) Welsh Ambulance Services National Health Service Trust

Effect

This amendment ensures that only police forces and security agencies may request a communications data warrant, except where the warrant is issued for the purpose of preventing death, in which circumstances emergency and rescue services also fall within the definition.

Amendment

Clause 62, page 50, line 22, delete clause 62

Effect

This amendment would prevent the Secretary of State from modifying clause 61 via Regulations.

Amendment

Clause 64, page 51, line 9, delete clause 64, 65, and 66

Effect

This amendment would delete the provision that states that local authorities are relevant public authorities for the purposes of the Bill and would delete associated clauses.

Briefing

As drafted, the legislation provides that all the bodies listed in Schedule 4 may access communications data under a system of internal authorisation. In addition to law enforcement and security agencies, this list currently includes certain Government Departments and other state bodies. The Bill explicitly defines local authorities as a relevant authority for the purposes of accessing communications data. The Bill also permits the Secretary of State to add to this list via regulations.

Digital Rights sets out that states must limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary. A long list of authorities, many of whose primary functions are wholly unrelated to law enforcement in the context of serious crimes, permitted to access this data is inconsistent with this requirement. Even more concerning is the fact that the legislation allows this list to be added to via Regulations, without the full and proper scrutiny of Parliament.

Filtering arrangements

Amendment

Clause 58, page 46, line 40, delete clause 58

Clause 59, page 47, line 36, delete clause 59

Clause 60, page 48, line 16, delete clause 60

Effect

These clauses would remove provisions for the establishment and use of a filter to gather communications data.

Briefing

The Bill contains provisions for a communications data 'Request Filter'[8] – a feature previously proposed in almost identical terms in the draft Communications Data Bill. The only change is that the Secretary of State must consult the Investigatory Powers Commissioner "*about the principles on the basis of which the Secretary of State intends to establish"* the filter.[9] The Request Filter is a search mechanism, allowing public authorities to conduct simple searches and complex queries of the databases that telecommunications operators are required to build and hold. The Joint Committee on the Draft Communications Data Bill described the 'Request Filter' proposed in that Bill as "*a Government owned and operated data mining device*",[10] which significantly positions the Government at the centre of the data retention and disclosure regime. Access to the Filter, and the data it produces, would be subject to the same self-authorisation process as all communications data. In practice, the 'Request Filter' would be a search engine over a "*federated database*"[11] of each and every citizen's call and text records, email records, location data, and now internet connection records, made available to hundreds of public authorities.

The Government is keen to portray the Request Filter as a 'safeguard' that "*will minimise the interference with the right to privacy".*[12] However, the processing of personal data represents a significant privacy intrusion. The Joint Committee on the draft Investigatory Powers Bill noted "*the privacy risks inherent in any system which facilitates access to large amounts of data in this manner".*[13] Whilst a useful tool for complex data searches, the 'Request Filter'

[8] Investigatory Powers Bill 2016, clause 58
[9] Investigatory Powers Bill 2016, clause 58, subsection (5); see also *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 232
[10] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 113, p.35
[11] Ibid.
[12] Draft Investigatory Powers Bill 2015: Explanatory Notes, p.23
[13] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 247

cannot be viewed as a straightforward safeguard. Rather it is a portal with power to put together a comprehensive picture of each of our lives. It raises many of the same concerns as a large and centralised store, with added security concerns of protecting multiple distributed databases.

Public authorities' permanent ability to access to the 'Request Filter' makes it an enticing and powerful tool that could be used for the broad range of statutory purposes - recently declared unlawful by the High Court.[14] The ability to conduct complex queries could increase the temptation to go on 'fishing expeditions': that is, to sift data in search of 'relationships' and infer that any concurrences are meaningful. This was one of the many concerns about this proposal expressed by the Joint Committee on the Draft Communications Data Bill.[15] For example, given this power, authorities could use communications data to identify attendees at a demonstration and correlate this with attendance at other public or private locations in the 12 month period; or to identify those regularly attending a place of worship, and correlate this with access to online radio websites, inferring risk.[16] Thus, this new ability could risk casting undue suspicion on thousands of innocent citizens.

[14] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin).
[15] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 126, p.37
[16] GCHQ appears to practice similar data mining on the basis of supposed risk factors: *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities* – Ryan Gallagher, The Intercept, 25 Sept 2015.

Whistle-blower protection

Amendment

Clause 73, page 58, line 34, insert new subsection (73)(4) –

(4) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the disclosure was in the public interest

Effect

This amendment would provide a defence to the criminal offence of disclosure in relation to a notice issued under this Part. The offence includes the disclosure of the existence of a notice. The offence is subject to a maximum penalty of two years imprisonment.

Briefing

By their very nature, surveillance powers are used in secret, with the vast majority of those subject to their use never realising that surveillance has taken place. This means that it is vital that there are in place sufficient checks, balances and safeguards to ensure that these powers are used appropriately. As part of this, it is essential to ensure that those who in one way or another witness or have knowledge that abuse or mistakes are taking place are able to bring those to the attention of individuals capable of addressing them. This may include bringing information to public attention.

Provisions in clause 73 which criminalise disclosure of information relating to the use of notices risk shutting down a vital route to ensuring accountability for the use of surveillance powers. They help to enshrine an unnecessarily secretive culture which punishes those who seek to reveal wrongdoing rather than encourage a robustly honest working environment. Individuals who wish to make reports – even internally – of unlawful or otherwise inappropriate behaviour will know that taking steps to do the right thing could expose them to criminal sanction. In a Bill that seeks to bring new levels of transparency to the UK's surveillance regime, this is clearly both undemocratic and unacceptable.

Confidential and privileged communications

Amendment

Page 54, line 1, delete clause 68 and insert new clause 68 –

Confidential and privileged communications

(1) Where a warrant is likely to cover communications data relating to individuals handling special procedure material, the procedure set out at section 3 below must be followed

(2) Where a warrant is likely to cover communications data relating to individuals handling excluded procedure material, the procedure set out at section 4 below must be followed

(3) Further to the requirements set out elsewhere in this part, the Judicial Commissioner may only issue a warrant if –

    (a) there are reasonable grounds for believing that an indictable offence has been committed, and

    (b) there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation in connection to the offence at (a), and

    (c) other proportionate methods of obtaining the material have been tried without success or have not been tried because they were assessed to be bound to fail, and

    (d) It is in the public interest having regard to:

        a. the democratic importance of freedom of expression under article 10 ECHR to grant the warrant; or

        b. the democratic interest in the confidentiality of correspondence with members of a relevant legislature; or

        c. the importance of maintaining public confidence in the confidentiality of material subject to legal professional privilege.

(4) Further to the requirements set out elsewhere in this part, the Judicial Commissioner may only issue a warrant in accordance with provisions made in Schedule 1 of the Police and Criminal Evidence Act and Schedule 5 of the Terrorism Act

(5) An application for a warrant under this Part must not be granted where the information could be sought using a warrant under schedule 1 PACE, unless seeking this information under PACE doing so would defeat the purpose of the investigation.

(6) Special procedure material means:

    a. Special material as defined in section 14 of the Police and Criminal Evidence Act 1984

b. Correspondence sent by or intended for a member of the relevant legislature

(7) Excluded material procedure has the same meaning as section 11 of the Police and Criminal Evidence Act 1984

(8) A warrant under this part may not authorise conduct undertaken for the purpose of accessing any communications data in relation to a communication, insofar as the communication relate to matters subject to legal privilege;

(9) For the purposes of subsection (8), legal privilege means –

(a) Communications between a professional legal adviser and his client or any person representing his client made in connection with the giving of legal advice to the client;

(b) Communications between a professional legal adviser and his client or any person representing his client and any other person with or in contemplation of legal proceedings or for the purposes of such proceedings;

(c) Items enclosed with or referred to in such communications and made:

i. In connection with the giving of legal advice or

ii. In connection with the contemplation of legal proceedings or for the purposes of such proceedings.

(d) Communications made with the intention of furthering a criminal purpose are not subject to legal privilege.

Effect

This amendment would replace the current, limited protection for communications data of journalists with a strengthened regime to protect the communications data of journalists, lawyers and Members of Parliament.

Briefing

Journalists generally have no protection in the Bill, and have no protection at all from interception, hacking, or any bulk powers. The one supposed safeguard is in clause 68, which would require a public authority to apply to a Judicial Commissioner to confirm an authorisation to obtain communications data if the stated purpose of access is to identify or confirm a journalistic source, However, this is a significant reduction of the well-established judicial process set out in the Police and Criminal Evidence Act 1984 (PACE), which as the NUJ has pointed out, protects not just the identity of sources but related journalistic material:

"Source protection does not just apply to the identity of the source but also to all matters relating to and communications between the journalist and the source. This

includes the person's name; personal data, voice and image. It also includes the unpublished content of information and the circumstances of acquiring the information".[17]

The Bill fails to define a journalist, and offers a questionable definition of journalistic sources (cl. 68(7)) that is unlikely to meet the standard set by recent case law from ECtHR[18].

In September 2014, it was revealed that the Metropolitan Police had used the RIPA internal authorisation route to access communications data of a journalist from The Sun newspaper as part of their "plebgate" inquiry, circumventing the well-established judicial process set out in the Police and Criminal Evidence Act 1984 (PACE). In response to public outcry, the Government updated the Acquisition and Disclosure of Communications Data Code of Practice, advising law enforcement that where an application to access the communications data of a journalist in order to determine the source of journalistic information is made, it must be via the PACE route. PACE sets out the special procedures that must be followed if law enforcement agencies wish to access material that may be journalistic or confidential journalistic material. To access journalistic material, which comes under the broad definition of *"material acquired or created for the purpose of journalism",* an application must be made to a judge. The conditions that must be met before the judge can grant a warrant include: that there are reasonable grounds for believing an indictable offence has been committed; the material is likely to be of substantial value; and, other methods of obtaining the material have been tried or are bound to fail. In addition to these requirements, the judge must be convinced that it is in the public interest to grant access to the materials. In order to access confidential journalistic material – namely information relating to sources – PACE sets out that a warrant will only be granted if prior to PACE it would have been possible to access source material via a power contained in primary legislation. As a result, it is only in very rare circumstances that an order will be made under PACE to reveal confidential journalistic material. Unlike the process contained in the Bill, both these processes are *inter-partes*, giving the journalist the opportunity to make their case to the judge. It is also possible to gain access to confidential journalistic material under the Terrorism Act 2000.

[17] *Written evidence on Investigatory Powers Bill* – NUJ, 21 Dec 2015
[18] *Guseva v Bulgaria* application no. 6987/07, 17 Feb 2015, para 38 and the cases cited.

The mechanism introduced by clause 68 is inadequate to secure the independence and vitality of our free press. It allows for a circumvention of the established and much more rigorous PACE process, creating a system in which communications data can be accessed without the PACE protections.

The Bill is also silent on the protection of communications data of lawyers. Legal privilege is an essential protection in a free society governed by the Rule of Law and is vital to uphold the right to a fair trial as protected by Article 6 of the European Convention on Human Rights. The doctrine is intended to ensure fair trial integrity and ensure both defendants and civil claimants can communicate with their lawyers without inhibition. Legally privileged communications are those between a client and their lawyer which come into existence for the dominant purpose of being used for legal advice, or in connection with actual or pending litigation. The Bar Council reminded the Joint Committee scrutinising the Bill that*, "The privilege is that of the client, and failure to protect that right against the state amounts to a significant inroad into a long-standing principle, which has formed an important foundation of our rule of law".* Without assured confidentiality, clients feel unable to speak openly with their lawyers and may not know about the proper defences available to them, thus obstructing a fair trial. Breaching privilege can also obstruct justice by jeopardising the integrity of criminal trials, or giving the state an unfair advantage. Legal privilege does not apply where client-lawyer communications are made in furtherance of a criminal activity.

The Government does not currently recognise that communications data come within the definition of legally privileged material. This is bizarre. It is clear that communications data may be in connection to the giving of legal advice and as such should be protected from state interference unless the communication is in furtherance of a criminal purpose. A phone call from or to a lawyer could, for example, identify potential witnesses in cases. The Bill therefore represents an important and timely opportunity to ensure statutory protection for LPP and to make clear that it extends to communications data.

Extraterritorial application

Amendment

Page 59, line 21, delete clause 76

Page 66, line 10, delete clause 86

Effect

These amendments would delete provisions which purport to give communications data access authorisations (authorisations and notices issued under Part 3) and data retention notices (notices issued under Part 4) extraterritorial effect.

Briefing

David Anderson's 2015 report "A Question of Trust" considered the matter of extraterritorial powers. Companies explained to the reviewer that they did not consider it was their role to arbitrate between conflicting legal systems. Liberty completely agrees: the protection of vital human rights should not be left to the goodwill and judgement of a company. The report also notes principled concerns from companies:

> *"They expressed concerns that unqualified cooperation with the British government would lead to expectations of similar cooperation with authoritarian governments, which would not be in their customers', their own corporate or democratic governments' interests."*[19]

The alternative, most appropriate – and probably most successful way – for Government to seek to access information held overseas or by companies based overseas is to extend and improve the use of Mutual Legal Assistance Agreements (MLATs) with other States. MLATs operate under the Crime (International Co-Operation) Act 2003 and allow for the sharing of information between States for the purposes of detecting and prosecuting crime. They provide a transparent framework, avoiding the legal complexities and human rights risks of States seeking to act unilaterally, leaving service providers as the only barrier against privacy violations. Not only do they offer the best way of ensuring that safeguards are applied internationally, but they have the capacity to be an extremely effective method for the transfer of information.

The report acknowledges that the MLAT system is currently slow and cumbersome, but concludes that the Governments should *"seek the improvement and abbreviation of MLAT*

[19] Paragraph 11.24.

procedures, in particular with the US Department of Justice and the Irish authorities" and *"take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations."*[20]

The report notes that US technology companies and civil society both advocated the improvement of MLATs as an alternative to extraterritorial provisions. The report also refers to the work of Sir Nigel Sheinwald as Special Envoy to the Prime Minister on law-enforcement and intelligence data sharing and suggests that Sir Nigel's will be *"the decisive voice"* on this matter. On 11 June, the Prime Minister's written statement responding to the Anderson review noted: *"the Government will be taking forward Sir Nigel's advice, including pursuing a strengthened UK-US Mutual Legal Assistance Treaty process and a new international framework. As David Anderson recognises in his report, updated powers, and robust oversight, will need to form the legal basis of any new international arrangements."*[21]

[20] Recommendation 24.
[21] House of Commons: Written Statement (HCWS27)

PART 4: COMMUNICATIONS DATA RETENTION

Amendment (to give warrantry powers to the Judicial Commissioner)

Clause 78, page 61, line 4, delete ‘Powers to require retention of certain data’ and insert ‘Power of Judicial Commissioners to issue data retention warrants’.

Clause 78, page 61, line 19, delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 30, delete ‘retention notice’ and insert ‘retention warrant’; delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 32, delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 33, delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 34, delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 36, delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 37, delete ‘notice’ and insert ‘warrant’.

Clause 78, page 61, line 38, delete ‘Secretary of State’ and insert ‘Judicial Commissioner’.

Clause 78, page 61, line 41, delete ‘notice’ and insert ‘warrant’.

Clause 79, page 62, line 26, delete ‘notice’ and insert ‘warrant’; delete ‘Secretary of State’ and insert ‘Judicial Commissioner’.
(Replace ‘notice’ with ‘warrant’ on lines 26, 28, 30, 31, 32, 33, 35).

Clause 79, page 62, line 35, delete ‘Secretary of State’ and insert ‘Judicial Commissioner’.

Clause 80, page 62, line 37, delete ‘Secretary of State’ and insert ‘Judicial Commissioner’.

Clause 80, page 62, line 38, delete ‘notice’ and insert ‘warrant’. (And repeat on lines 41, 42)

Clause 80, page 62, line 40, delete “Secretary of State’ and insert ‘Judicial Commissioner’

Clause 80, page 63, line 5, delete ‘notice’ and insert ‘warrant’. (And repeat on lines 6, 7, 8, 14, 16, 27, 28, 30, 33)

Clause 80, page 63, line 7, delete ‘Secretary of State’ and insert ‘Judicial Commissioner’. (And repeat on lines 8, 10, 19, 24, 25, 31, 33).

Clause 83, page 64, line 13, delete “Secretary of State’ and insert ‘Judicial Commissioner’. (And repeat on lines 14, 15, 23, 38, 40, 41).

Clause 83, page 64, line 11, delete ‘notices’ and insert ‘warrants’. (And repeat on line 12).

Clause 83, page 64, line 13, delete ‘notice’ and insert ‘warrant’. (And repeat on line22, 27, 28, 31, 32, 34, 36, 37, 39; and on page 65, line 7, 9).

Effect

These amendments would remove the role the Secretary of State to issue data retention orders and instead provide for Judicial Commissioners to issue data retention warrants.

Amendment (to provide for application for a warrant)

Clause 78, page 62, line 23, insert new clause 78A –

(78A) Persons who may apply for issue of warrant

(1) Each of the following organisations may apply for a communications data retention warrant -

(a) A police force maintained under section 2 of the Police Act 1996
(b) Metropolitan police force
(c) City of London police force
(d) Police Service of Scotland
(e) Police Service of Northern Ireland
(f) British Transport Police Force
(g) Ministry of Defence Police

(h) Royal Navy Police
(i) Royal Military Police
(j) Royal Air Force Police
(k) Security Service
(l) Secret Intelligence Service
(m) GCHQ
(n) National Crime Agency

Amendment (to limit the purposes for which a data retention warrant may be issued)

Clause 78, page 61, line 5, delete subclause (1) and insert new subclause (1) -

(1) A Judicial Commissioner may issue a data retention warrant under this Part to authorise the retention of relevant communications data if the Judicial Commissioner considers that the authorisation is necessary and proportionate for one or more of the following purposes -

(a) in the interests of national security, or

(b) for the purpose of preventing or detecting serious crime, where there is reasonable suspicion that a serious criminal offence has been or is likely to be committed, or

(c) for the purpose of preventing death or injury.

Clause 78, page 61, line 10, delete 'A retention notice may' and insert 'A data retention warrant must'.

Clause 78, page 61, line 11, delete 'or any description of'

Clause 78, page 61, line 11, delete 'of all data or any description of data' and insert 'of specified relevant communications data'

Clause 78, page 61, line 14, delete subclause (2)(d)

Clause 78, page 61, line 16, delete subclause (2)(e)

Clause 78, page 61, line 37, delete '(or description of operators)' and insert 'or operators'.

Clause 78, page 61, line 39, delete '(or description of operators)' and insert 'or operators'.

Clause 78, page 61, line 42, delete ‘(or description of operators)’ and insert ‘or operators’.

Clause 80, page 62, line 42, delete subclause (3)

Clause 83, page 64, line 16, delete ‘(or description of operators)’ and insert ‘or operators’. (And repeat on page 65, lines 1, 8, 10).

Effect

These amendments would provide for clear, appropriate and limited grounds on which data retention warrants may be issued to help an investigation or operation. The grounds amended for here reflect those recommended for communications data access authorisations.

These amendments require that the data to be retained is specified.
These amendments also require that warrants to retain communications data on organisations require those organisations to be identified rather than merely described.

Safeguards for communications data retention warrants

Amendment
Clause 72, page 57, line 36, delete subclause (2)(b)

Amendment

Page 62, line 25, insert new clause 79 A –

> Requirements that must be met by warrants
>
> (1) A warrant issued under this Part must name or otherwise identify the person or persons, organisation, premises, or location to which the warrant relates.
>
> (2) A warrant issued under this Part must describe the investigation or operation to which the warrant relates.

(3) A warrant issued under this Part must relate to one or more of the following purposes -

(a) in the interests of national security, or

(b) for the purpose of preventing or detecting serious crime, where there is reasonable suspicion that a serious criminal offence has been or is likely to be committed, or

(c) for the purpose of preventing death or injury.

(4) A warrant may only be issued under this Part if there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation or operation to which the warrant relates.

Effect

These amendments would require that data retention notices are issued only for specific investigative or operational purposes, to obtain specified data, where the data is believed to be of substantial value.

Briefing

Part 4 gives the Secretary of State the power to issue a retention notice to require telecommunications operators to retain all communications data for up to twelve months. Communications data is defined as data which may be used to identify or assist in identifying the sender, recipient, time, duration, type, method, pattern, or fact of a communication, along with system used to make a communication, its location and the IP address or other identifier of any apparatus used. Liberty supports the important role of communications data in missing persons situations, preventing and investigating serious crime. We do not believe however that the role of communications data in the investigation of crime justifies a Secretary of State mandate for blanket retention of the historic communications data of the entire population for 12 months.

Instead of the Secretary of State imposing an arbitrary and speculative data retention notice covering the whole population, we propose that police forces should be able to apply to a Judicial Commissioner for targeted data retention warrants where data is required for the purposes of a specific investigation into serious crime or for the purpose of preventing death or injury.

A significant amount of data is already retained by telecommunications operators for their business purposes. Where a warrant under this part is not in place, that data may still be sought using an access warrant under Part 3.

Internet connection records

Amendment

Clause 78, page 62, line 22, delete 'and this expression therefore includes, in particular, internet connection records'.

Effect

This amendment would remove the requirement for 'internet connection records' to be retained by ISPs.

Briefing

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. Under current legislation in DRIPA 2014, public telecommunications operators may be required to retain "*relevant communications data"* for up to 12 months[22], including data that may be used to identify the internet protocol (IP) addresses of senders and recipients of communications. However, this 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.[23]

ICRs are described in the Bill as communications data which "*may be used to identify, or assist in identifying, a telecommunications service".*[24] In explanatory notes accompanying the draft Bill, ICRs are described as "*a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet".*[25] However, the exact fields of information that would constitute an ICR have not been defined.

A plethora of public authorities will 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.[26] The scale of public authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access.

---

[22] *Data Retention and Investigatory Powers Act 2014,* section 1

[23] *Counter Terrorism and Security Act 2015,* section 21(3)(c)
[24] *Investigatory Powers Bill 2016,* clause 54, subsection (6)(a)
[25] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.29
[26] *Investigatory Powers Bill 2016,* schedule 4, part 1

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 relating to suspects will mirror existing provisions for access to communications data and instead be authorised by a 'designated person'[27] within the public authority, and then by a 'single point of contact.'[28]Provisions in the Bill would permit law enforcement and public authorities to gain access to ICRs for four purposes: to identify who or what device has sent a communication or used an internet service; to identify what internet communications services have been used, when and how; to identify when and where a person has accessed or made available illegal material; and now in the revised Bill, the additional power to reveal all internet connections of an identified person.[29]

Defining ICRs

ICRs do not naturally exist within the technical infrastructure of a telecommunications operator. The Bill and accompanying documents have consistently failed to define the exact fields of information that would constitute an 'internet connection record' – indeed, 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'[30], and the draft Code of Practice confirms that 'there is no single set of data that constitutes an internet connection record'.[31] The Home Office's accompanying ICR factsheet says that ICRs "*will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date*".[32] The Home Office was pressed to release further evidence to define what would be collected as 'communications data' including ICRs to the Joint Committee. It released an annex of 'examples' which revealed not only web addresses and IP addresses are included, but the names, addresses, email addresses, phone numbers and billing data of customers; usernames and passwords; locations of internet access and each internet communication; and device identifiers (MAC address, IMSI, IMEI).[33].

[27] *Investigatory Powers Bill 2016,* clause 53
[28] *Investigatory Powers Bill 2016,* clause 67. A SPoC is an "*accredited*", "*trained*" individual. *Investigatory Powers Bill: Explanatory Notes,* 4 Nov 2015, p. 27
[29] *Investigatory Powers Bill 2016,* clause 54, subsection (4)
[30] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.1
[31] *Communications Data: Draft Code of Practice* – Home Office, 1 March 2016, p.18
[32] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[33] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.6

"*The voice of the internet industry"*, the Internet Service Providers Association (ISPA) expressed concern that ICRs have not been properly defined.[34] The Joint Committee reported, "*We have concerns about the definitions and feasibility of the existing proposal, which the Home Office must address".*[35] Widespread concerns from major tech companies in response to the Home Office's incompetent ICRs proposals led the Committee to recommended 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."*[36] The Science and Technology Committee's press release stated, "*The Bill was intended to provide clarity to the industry, but the current draft contains very broad and ambiguous definitions of ICRs, which are confusing communications providers."*[37] However, no further clarity or definition has been provided in the revised Bill or accompanying documents.

In practice, 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.

Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways. First, they can request telecommunications operators to retain the data of specific targets on a forward-looking basis.[38] Secondly, they can request retrospective 'internet connection' data on specific targets from operators who temporarily store it for their own business purposes.[39] 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.[40] 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[41]. 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*

---

[34] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015
[35] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 106
[36] Ibid. Recommendation 7, para. 122
[37] *Press Release: Cost of Investigatory Powers Bill Could Undermine UK Tech Sector* – Science and Technology Committee, 1 February 2016
[38] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.25
[39] *Operational Case for the Retention of Internet Connection Records,* 2015, p.25
[40] *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
[41] *GCHQ and NCA join forced to ensure no hiding place online for criminals* – NCA, 6 Nov 2015

other capabilities which enable them to obtain equivalent data."[42] The ISC recommended that this be amended in the Bill "*in the interests of transparency*"; yet no such transparency has been provided.

Liberty believes the case supporting this expanded data collection by ISPs, including its claimed benefit to law enforcement, is deeply flawed, contradicted by the available evidence, and has been accurately described as "*overstated and misunderstood*".[43] Further, there is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[44]. 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.[45] As the CJEU ruled in 2014,[46] 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.

Access to ICRs will be granted for the furtherance of one of four purposes. However, the need for further powers in relation to each of these purposes is flawed.

Rebuttal to Purpose 1: Identifying the individual device that has sent a communication online

The Metropolitan Police and National Crime Agency (NCA) have suggested that without ICRs, they cannot resolve IP addresses (that is, identify web users) and continue investigations in a minority of cases (approximately 14%[47]).

In the *Operational Case for the Retention of Internet Records*, published with the draft Bill, three case studies of discontinued investigations relating to child sexual exploitation and three relating to fraud are presented to support the argument for retaining ICRs. It is claimed that ICR retention would be required in order to progress those investigations and increase chances of accurately identifying a web user.[48] However, the likelihood of bulk ICRs to prove vital in accurately identifying otherwise anonymous suspects of serious crime has been

---

[42] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation I.
[43] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[44] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[45] Ibid
[46] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014
[47] It is argued that the retention of ICRs would improve the chances of being able to resolve an IP address in 14% of cases in a sample from the US based National Centre for Missing and Exploited Children, NCMEC - as cited in the ICR evidence base: *Operational Case for the Retention of Internet Connection Records,* 2015, p.14
[48] *Operational Case for the Retention of Internet Connection Records,* 2015, p.20

questioned by ISPs and technologists.[49] The justification relies on the assumption that online criminals offend using a regular browser or public file sharing service on their own device, using personal internet connections, 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. Furthermore, the retention of ICRs will push internet traffic, both legitimate and otherwise, into more protected spaces. This inevitable digital shift will render ICRs an invasive database of, almost exclusively, innocent citizen's digital lives, and forced retention of them a costly, out-dated, ineffective strategy.

In the limited cases where the ICRs might assist in resolving an IP address they will provide limited assistance in identification of suspects as they can only help to identify a device, such as a laptop or PC – not an individual user. Identifying a specific user requires a context of information that would typically be gathered in a targeted surveillance operation. Devices such as laptops, PCs, tablets and even smart phones are commonly shared within families, workplaces and public institutions, further diminishing the value of bulk ICRs in identifying an individual suspect. Indeed, ICR data is "inexact and error-prone".[50]

In evaluating the efficacy of ICRs in serving the purpose of IP resolution and identification of a suspect, 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. Denmark's data retention law compelled telecommunications operators to store internet session data for 12 months including client and server IP addresses, port numbers, transmission protocols and timestamps.[51] The data retention excluded DNS logs (i.e. the names of the websites the server IP addresses corresponded to). **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**

[49] *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

[50] *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

[51] *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

minimal role in only one case.[52] In fact, Ministry staffers reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[53] In 2013, approximately 3,500 billion telecommunication records were retained in Denmark, averaging 620,000 records per citizen.[54] 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*".[55]

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.[56] Despite the rhetoric of "*important differences"*, there are two differences in substance. Firstly, the UK Government promises (although will not make a statutory commitment) to meet CSPs' costs upfront to cover the necessary infrastructural change, drain on resources, and generation and storage of data – whereas in Denmark, CSPs were paid for the generation and storage of data after they implemented infrastructural change. It does not follow that this different mode of reimbursement will affect the usability of data. 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 exert an unprecedented level of control over CSPs through 'negotiations' which it anticipates will provide for never-before-seen modes of tailored data collection at the population level. These proposals have proved deeply unconvincing, unpopular, and even alarming to CSPs.[57]

---

[52] *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).

[53] Ibid.

[54] *Written evidence on Investigatory Powers Bill: Technology Issues* - IT-Political Association of Denmark, 2 Dec 2015, p.2

[55] *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

[56] *Comparison of internet connection records in the Investigatory Powers Bill with Danish Internet Session Logging legislation* – Home Office, 1 March 2016

[57] See written and oral evidence to the Joint Committee and the Science and Technology Committee.

Rebuttal to Purpose 2 - identify what ISPs an identified suspect has used, when and how[58], in order to inform law enforcement as to which communications service providers to request further information from.

The second part of the Home Office's case for mass ICR retention rests on the idea that this is required to help inform law enforcement request further information on identified suspects. This argument overlooks the range of intrusive powers already on the statute book. It is far more preferable, from both a human rights and law enforcement perspective, to employ robust targeted powers on identified suspects than intrude on the rights of the entire population. Existing powers for obtaining further information about communications of suspects include: using targeted interception, making targeted requests for communications data from service providers, and seizing and forensically examining a device. However, the Home Office presents these targeted approaches as less favourable than the mass retention of ICRs.

The argument in favour of this new, invasive category of bulk data retention rests, in part, upon the claim that there is an "*extremely high threshold"*[59] and "*very limited circumstances in which the interception of communications content can be authorised*", and therefore targeted interception "*cannot be used in most law enforcement cases".*[60] This is a peculiar argument, as interception is used for three broad statutory purposes: the prevention and detection of serious crime (which accounts for 68% of interception warrants[61]), the interests of national security and for the economic well-being of the UK.[62] The case studies provided to support the case for ICR retention all qualify as serious crimes[63] for which interception can be used, as they relate to child sex abuse, fraud and human trafficking.

Additionally, it is claimed that law enforcement bodies cannot request data from popular online service providers who store communications data for their own purposes, such as Facebook, without ICR evidence proving that the individual or device in question definitely accessed their service.[64] Without this data, they argue that such a request "*is unlikely to be necessary and proportionate*".[65] Liberty does not recognise this explanation. If the authorities have objective and reasonable grounds for suspecting serious criminality and further believe

[58] *Draft Investigatory Powers Bill 2015,* clause 47 (4)(b)
[59] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17
[60] *Operational Case for the Retention of Internet Connection Records,* 2015, p.16
[61] *HM Government Transparency Report 2015: Disruptive and Investigatory Powers,* p.34
[62] *Draft Investigatory Powers Bill 2015,* clause 14 (3)
[63] Serious crimes are those that incur a sentence of 3 years or more; violent crimes; crimes involving substantial financial gain, or conduct by a large number of persons in pursuit of a common purpose. *Draft Investigatory Powers Bill 2015,* clause 195 (1),
[64] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4; p.25
[65] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4

that the suspect's use of a telecommunications platform may provide evidence of the offence, a request for communications data will be necessary and proportionate.[66] If the suspect did not use the communications service, the data would simply not be there to obtain.

As a third argument for ICR retention, law enforcement bodies say it is "*thanks to seizure of devices*" that it has thus far been possible to identify communications services used by suspects, but that seizure of a device "*will not always be the preferred course of action in an investigation, as it is an overt action that will normally involve an arrest*".[67] Investigators would rather "*develop intelligence on the group covertly*" and establish any possible "*previous linkages"* between group members. However, links between group members can be covertly discovered through a targeted communications data retention order; through requests for retrospective data from the operators who store it for their own purposes; or through interception.

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 smartphone app or social media website prior to his or her disappearance".*[68] In response, ISPA (Internet Service Providers Association) members *"pointed out the huge flaw in this argument*".[69] 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) often stays connected in the background whether in current use or not, remaining connected for a period of days, weeks or months.[70] Connection records show connection timestamps rather than access timestamps, and one such 'internet connection' could exceed the 12 month retention period by the time it is logged. ISPs and technologists have expressed serious concern that the Home Office has based an extensive,

---

[66] Many online public services are co-operative with law enforcement: Facebook, for example, co-operates with the NCMEC and has an established system for law enforcement data requests[66]. In the period January 2015 – June 2015, UK law enforcement made 3,384 requests to Facebook alone for various types of data, relating to 4,489 accounts; Facebook found legal basis to comply with 78.04% of these requests[66].

[67] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17

[68] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015

[69] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html

[70] 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.

invasive data collection policy on a fundamental misunderstanding, or worse misguidance, as to how internet connections work, and that it has provided misleading descriptions of what purposes ICRs would serve accordingly.

Rebuttal to Purpose 3 - to "identify the accessing of illegal online services or websites"[71]*.*

The value of ICRs in consistently and accurately identifying access to illegal websites has also been over-estimated and misunderstood. The bulk collection 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 generate a separate 'internet connection', which may relate to a server 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. Bulk ICR retention could be exploited by hackers for nefarious purposes – for example, by embedding 'suspicious' scripts into webpages, 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. 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.

Rebuttal to Purpose 4 – to view any "internet services (websites, apps, etc.) *an individual is using"*

The three purposes described above, provided as the original justification for the collection of ICRs, are now largely unnecessary, as the revised Bill has expanded the police and public authorities' power to access all of an individuals' ICRs[72] – not just those relating to "*internet communication services*" or "*illegal online services"* . This is not only unnecessary, but alarmingly disproportionate. In 2014, there were 517, 236 authorisations for public authorities' access to communications data.[73] 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.

---

[71] Draft Investigatory Powers Bill 2015, clause 47 (4)(c).
[72] Investigatory Powers Bill 2016, clause 54, subsection (4)(d)
[73] *Statistics: Communications Data* – IOCCO, http://www.iocco-uk.info/sections.asp?sectionID=12&type=top, retrieved 10 March 2016

Threat to privacy and 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 "*honeypot for casual hackers, blackmailers, criminals large and small from around the world and foreign states*".**[74] 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*".[75] The Joint Committee on the draft Investigatory Powers Bill noted that "*data theft remains an ongoing challenge".*[76] 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,[77] it is extraordinarily irresponsible to coerce private companies with the burden of generating, storing and securing 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.[78] 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 Anderson pointed out in his independent review.[79]

---

[74] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.
[75] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, pp.28-29
[76] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Para. 174
[77] 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.
[78] Investigatory Powers Bill 2016, clause 86
[79] A Question of Trust: Report of the Investigatory Powers Review – David Anderson Q.C., June 2015, p.207

The difficulty of tracking some online criminals is a real problem. However, it is not a problem that mass surveillance programs – least of all this one - can solve. Bulk ICR retention will not be able to meet these three investigative purposes with 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 reluctant telecommunications operators to spy on their customers would be better spent on hiring more officers to conduct targeted, warranted surveillance on suspects of serious crime.

Sara Ogilvie

Silkie Carlo