PRIVACY INTERNATIONAL

LIBERTY80
PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

ARTICLE 19

ENGLISH PEN

Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN briefing on the fast-track Data Retention and Investigatory Powers Bill

Introduction

1. The Data Retention and Investigatory Powers (DRIP) Bill was published on 10th July 2014 following a press conference given by the Prime Minister and Deputy Prime Minister announcing emergency surveillance legislation. They indicated that the leader of the Opposition had already given Labour's support to the Bill following private cross-party discussions and this was confirmed by the Shadow Home Secretary in the Chamber later in the day. The Bill is now due to receive all its substantive stages in the House of Commons next Tuesday 16th July. The Lords will be invited to pass the Bill on Wednesday and the Commons will consider any Lords amendments on Thursday. Royal Assent is to be granted before summer recess and the legislation will come into effect immediately. Parliamentary scrutiny and debate is therefore effectively neutered and it is unlikely that the Bill will be substantively amended.

2. In introducing this legislation, the security services, civil service and Coalition and the Opposition leaders have demonstrated a staggering disregard for parliamentary democracy and the Rule of Law. If there is any opportunity for amendment we recommend that the Bill's sunset is brought forward to reflect its supposedly temporary nature. The Bill is currently due to expire on 31 December 2016 – two and a half years away. Given widespread public, international and commercial concern about the Government's surveillance powers (which are significantly extended here) and the likely unlawful nature of at least part of the Bill's substance, we strongly advise parliamentarians to amend the sunset expiry date to 31 December 2014. This will at least ensure that RIPA review takes place in a timely manner and Parliament is able to reassert its constitutional function.

The Bill

3. The Government says that the need for the Bill is twofold. First to respond to the judgment of the Grand Chamber of the Court of Justice of the European Union (CJEU) in the joined cases brought by *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12) handed down on 8 April 2014. And secondly to 'clarify' the extra-territorial reach of the *Regulation of Investigatory Powers Act 2000* (RIPA).

4. The Bill proposes sweeping new surveillance powers. Most significant are clauses 1 and 4. Clause 1 provides powers to re-enact the Data Retention (EC Directive) Regulations 2009 that were nullified as a result of the CJEU judgment. Clause 2 contains relevant definitions. Clause 3 slightly amends one of the purposes for which interception warrants can be issued and communications data can be obtained under RIPA. Clause 4 grants significant new powers that extend the territorial scope of the broad interception and communications acquisition powers under RIPA. The powers in clause 4 (taken with clause 5) not only appear to deliver data access powers the Government previously sought via the Draft Communications Data Bill, they also appear to extend significantly the Government's interception capabilities by enabling the service of interception warrants and orders requiring the maintenance of interception capabilities to entities outside the United Kingdom.

5. Although the Bill has been posited as addressing the problem of retention of and access to communications data, in fact it is very clear that the Bill pertains to the powers of the Government to access communications content. In extending the territorial reach of the RIPA interception regime, the Government seeks to dramatically expand its ability to mandate the interception of communications content across the globe.

No need for fast track legislation

6. The Government claims that a sudden emergency has arisen, justifying fast-track legislation. This is not the case. The CJEU judgment was handed down over 3 months ago and well before the Queen's Speech in May this year. The Government has had ample time to bring forward legislation in the usual way if it so wished. Further, a number of our organisations wrote to the Home Secretary in April, drawing her attention to the judgment and stating our view that the judgment nullifies the Regulations. The Home Office responded in May with its view that the Regulations remain legally in force and explaining that service providers in receipt of a notice under the Regulations had been advised that they should continue to observe their notice obligations. No action was taken to address the implications of the judgment, and there is therefore no reason why emergency legislation can be justified now.

The extension of powers currently under judicial scrutiny

7. The Bill purports to significantly extend the scope of interception powers under RIPA, which are currently under scrutiny by the Investigatory Powers Tribunal (IPT). Next week the Secretary of States for the Foreign and Commonwealth Office and the Home Office, along with the Secret Intelligence Service, the Government Communications Headquarters and the Attorney General will answer claims that the RIPA interception regime violates Articles 8 and 10 of the European Convention of Human Rights (ECHR). Liberty, Privacy International and others contend that RIPA interception powers have been used to conduct bulk indiscriminate surveillance of communications as they enter and leave the United Kingdom. This Bill expands those same powers, appearing to enable the Government to issue interception warrants mandating mass surveillance outside of the United Kingdom.

Clauses 1 & 2: Communications Data Retention

Implications of the Digital Rights Ireland case

8. The EU Data Retention Directive 2006/24/EC imposed an obligation on Member States to adopt measures to ensure that communications data generated or processed by providers of public communications services or networks within their jurisdiction be retained for 6-24 months and stored in such a way that it could be transmitted upon request to the 'competent authorities' without delay. Implementation of the Directive in UK law was achieved through the Regulations in force on 6th April 2009. The Regulations created the power for the Home Secretary to require communication service providers to retain communications data that they already held for business purposes for a prescribed period of 12 months.

9. The *Digital Rights Ireland* case ruled on the validity of the Directive following a referral by the High Court of Ireland and Verfassungsgerichtshof (Constitutional Court, Austria). The CJEU declared the Directive to be invalid as its provisions were incompatible with the rights guaranteed under Articles 7 & 8 and 52(1) of the Charter of Fundamental Rights of the European Union[1] It concluded that the Directive entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference

[1] Article 7 of the Charter of Fundamental Rights & Freedoms protects Respect for Private and

being limited to what is strictly necessary. The Court found that the EU legislature had "*exceeded the limits imposed by compliance with the principle of proportionality."*[2]

10. The domestic effect of the judgment is twofold: both procedural and substantive. First, the CJEU judgment nullifies the Regulations. The Regulations were made pursuant to the power in section 2(2) of the European Communities Act 1972 which gives Government the power to make provision for implementing any "EU obligation". As the EU obligation no longer exists, the Regulations are therefore *ultra vires* or in other words beyond power and invalid. Second, the CJEU identified several characteristics of the Data Retention Directive that rendered the regime disproportionate. The effect of this was to define the limits of permissible data retention pursuant to human rights law and EU law. It is for the Government to demonstrate that any new proposal is proportionate in light of the CJEU's findings.

11. Any legislation mandating data retention by a Member State of the EU therefore now must comply with the following ten principles –

1. 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);
2. provide exceptions for persons whose communications are subject to an obligation of professional secrecy (paragraph 58);
3. distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
4. ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);
5. 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);
6. restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);
7. limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);

[2] Digital Rights Ireland case, para 69.

8. ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access (paragraph 66);
9. ensure destruction of the data when it is no longer required (paragraph 67); and
10. ensure the data is kept within the EU (paragraph 68).

Effect of Clause 1

12. Clause 1 of the DRIP Bill doesn't even pretend to comply with the CJEU judgment. Instead it seeks to re-enact a regime which would allow for mandatory blanket communications data retention of the entire population for up to 12 months without any nexus to the prevention or detection of serious crime, nor the other privacy safeguards laid out in the judgment. Under clause 1 the Home Secretary will continue be able to mandate, by order, the retention of 'relevant communications data' including 'all data'[3] for a period of up to 12 months[4] for any of the broad purposes set out in section 22(2) paragraphs (a) to (h) of RIPA which include for example the assessment of taxes and the prevention of disorder.

13. The Bill also fails to narrow the loose and lax communications data access regime for public authorities' provided by Chapter 2 of RIPA and under the section 25(1) *Regulation of Investigatory Powers (Communications Data) Order 2010*. The law currently authorises the acquisition of communications data by hundreds of public authorities and most public bodies are able to authorise internally their access to communications data for the same broad range of purposes under which communications data is retained. Barring local authority access, there is no requirement for independent prior judicial authorisation when communications data is sought by public bodies.[5]

14. In light of the woefully inadequate access regime under RIPA, the DRIP Bill's silence on access will allow for ongoing wide scale privacy infringement. Since the 2009 Regulations have been in force, communications data has been accessed on a massive scale in the UK with roughly half a million requests from public bodies per year. The rules governing targeted surveillance make it impossible to know with any

[3] Clause 1(2)(b).
[4] Clause 1(5).
[5] Section 37 of the *Protection of Freedoms Act 2012* introduced a requirement for prior judicial authorisation for access to communications data by local authorities. The Government has offered no explanation as to why this safeguard should not be mandatory for all communications data access requests.

certainty the scale of disproportionate use and abuse of communications data by public authorities but the sheer volume of requests and inadvertent examples of bad practice make clear that it is a serious problem.[6] In 2013, 869 communications data errors were reported to the Interception of Communications Commissioner and a further 101 identified during his random inspections.[7] Several errors had "*very serious consequences*" including warrants being *"executed at the homes of innocent account holders and this is extremely regrettable."*[8]

15. The Bill's explanatory notes make no effort to identify what is required to comply with the CJEU judgment and instead blithely assert *"The judgment of the ECJ raised a number of issues concerning the Data Retention Directive. Many of these were already met by the safeguards within the UK's comprehensive data retention and access regime. Nevertheless where appropriate the Bill adds safeguards while providing for the replacement regulations to add further safeguards in line with the judgment".*[9] The only apparent concessions made to the judgment are that in issuing a retention notice the Home Secretary must consider the requirement is necessary and proportionate[10] and the period of retention is set at a maximum (rather than fixed) 12 months. The necessity and proportionality requirement offers little comfort in light of the Government's apparent refusal to accept that blanket retention is disproportionate and on its face the Bill still continues to allow for blanket mandatory retention for all communications data for 12 months. Clause 1(3) and (4) provide for secondary regulations (published in draft on 11th July) to make further provision about the retention of communications data. However, given the sweeping mandatory retention powers contained on the face of the Bill, regulations will be unable to secure compliance with the criteria of the CJEU. This is confirmed by the substance of the draft regulations.[11]

---

[6] A freedom of information request involving Humberside police revealed that a residual category for communications data access requests is 'other non-crime'.
[7] Annual Report of the Interception of Communications Commissioner 2013, para 4.48, published April 2014.
[8] Ibid at para 4.51
[9] Explanatory notes, paragraph 11.
[10] Clause 1(1).
[11] Provisional draft of the Data Retention Regulations 2014, 11 July 2014 available at - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/329785/Provisional-DRR2014-with-cover-sheet.pdf.

Private nature of communications data

16. Communications data can disclose the date, time, duration and type of communication, the type of communication equipment used, its location, the calling telephone number, the receiving telephone number and the IP address for email internet services. 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 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.*"[12] Furthermore, consider the range of situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a Times reporter immediately before a major whistle-blower scandal fills the 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.

17. The Government seeks to diminish the importance and sensitivity of communications data by distinguishing it from the content of communications, accessed via RIPA's interceptions provisions. At one time a firm distinction between communications data and content would have been more credible, for example when much communication was 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 and it is now well established that modern-day communications data can provide a deeply intimate picture of a person's life and deserves a presumption of protection.

Continuing and unlawful breach of human rights

18. Clause 1 is incompatible with human rights for the same reasons that the Directive was found unlawful under Charter of Fundamental Rights. While the Directive was challenged on the basis of Charter rights because it was EU legislation, Article 8 of the ECHR contains a parallel right to those contained in Articles 7 & 8 of

[12] Digital Rights Ireland case, para 27.

Charter[13] and unless new legislation takes account of the substance of the CJEU judgment it will be open to immediate legal challenge under the *Human Rights Act 1998*. This will return the Government to its present predicament.

19. Government relies on use of communications data in counter-terrorism operations and a number of high profile cases to justify blanket retention. In presenting these cases, no detail is provided about the role of historic communications data in investigation and whether prosecutions could have been secured without access to data retained for 12 months. Widespread use of communications data in criminal investigations is unsurprising given that blanket data on the entire population is currently retained and public authorities are able to access the data with ease. This does not mean that the current scale of communications data use is either necessary or proportionate. In 2013, public authorities submitted 514, 608 requests for communications data which the new Interception of Communications Commissioner has warned "*seems to me to be a very large number. It has the feel of being too many*".[14] In light of his concerns he has asked his inspectors to take a critical look at the scale of requests due to fears of "*significant institutional overuse of the Part 1 Chapter 2 powers. This may apply in particular to police forces and law enforcement agencies who between them account for approaching 90% of the bulk*".[15]

20. Blanket data retention has been held superfluous, harmful or even unconstitutional in many States across Europe, including in Germany,[16] Romania,[17]

[13] Article 8 of the ECHR provides that everyone has the *right to respect for his private and family life, his home and correspondence.* The ECHR is incorporated into UK law by the *Human Rights Act 1998.*
[14] Footnote 7, Para 4.28.
[15] Ibid.
[16] In March 2010, Germany's Constitutional Court declared the provisions of its law transposing the Directive unconstitutional. In finding the communications data retention regime incompatible with constitutional protection for personal privacy, the Court commented that *'the protection of communication does not include only the content but also the secrecy of the circumstances of the communication, including if, when and how many times did some person…contact another. The Court went on to find that 'the evaluation of this data makes it possible to make conclusions about hidden depths of a person's private life and gives under certain circumstances a picture of detailed personality and movement profiles; therefore it can not be in general concluded that the use of this data presents a less extensive intrusion than the control of the content of communications. B*undersverfassungsgericht, 1 BvR 256/08. English press release at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html (judgment only in German)
[17] In October 2008, the Romanian Constitution Court became the first to declare legislation transposing the EU Directive in breach of its Constitution. The Court found that the mandatory retention of communications data scheme engaged a number of fundamental rights, namely the right to freedom of movement, the right to intimate, family and private life, privacy of correspondence and the right to freedom of expression. In finding its transposing legislation

Bulgaria,[18] Belgium, Austria, Sweden and Greece. The unconstitutional nature of blanket retention of modern communications data has also recently been recognised by a US federal judge in a ruling that may ultimately put an end to the NSA's bulk metadata collection on US citizens. In December 2013 US District of Colombia Judge Richard J Leon found that a lawsuit challenging NSA bulk metadata collection demonstrated a "substantial likelihood of success".[19] Describing the nature of modern-day metadata US federal Judge Leon said "*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."*

21. Just as the judgment in *S and Marper v UK*[20] required a new policy on police retention of innocents' DNA so too does the CJEU judgment require a new policy on the retention of innocents' communications. In response to *S and Marper* the Government legislated for a new policy and has undertaken the deletion of over 1 million DNA profiles. Yet no attempt has been made to explain or justify the different approach it takes here. The explanatory notes contain just one tautological sentence on the question "*The measures are in pursuit of a legitimate aim and proportionate to that aim. Accordingly the measures concerning data retention are in accordance with Article 8 of the Convention."*[21]

Clause 4: Extra-territorial interception and communications data acquisition powers

22. Clause 4 creates new powers for the extra-territorial reach of the interception warrants, orders relating to the maintenance of interception capability and

---

disproportionate, the Court relied on, amongst other issues, the reversal of the ordinary presumption of innocence and the lack of a reasoned basis for the retention period required, finding also that retention on the scale required was *'likely to prejudice, to inhibit the free usage of the right to communication or expression'.* Decision no 1258 of the Romanian Constitutional Court, 8 October 2009. Available at: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

[18] In 2008 the Bulgarian Supreme Administrative Court, found the legislation implementing the Eu Data Retention Directive incompatible with the country's constitutional protection of personal privacy.

[19] 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-judge-rules-nsa-program-is-likely-unconstitutional/668/.

[20] *S and Marper v United Kingdom* [2008] ECHR 1581.

[21] Explanatory Notes, page 15.

communications data acquisition requests under RIPA. While the Government says it seeks to "clarify" the extraterritorial reach that it believes has always been implied, these are very clearly new powers not previously provided for in legislation. In fact, these powers drastically increase the Government's authority to intercept communications, purporting to extend globally the UK's ability to mandate interception assistance. Under these powers, overseas companies may be made subject to the wide powers in RIPA, which are already under challenge before the British courts.

23. Clause 4 gives interception warrants extra-territorial effect. At clause 4(2) of the Bill, the Government purports to require companies based overseas – including foreign telecommunications companies as well as internet services - to comply with interception warrants that were previously issued only in relation to UK providers. Copies of these warrants would be served on foreign companies co-opting them into the provision of interception capability to our Government.

24. DRIP will therefore significantly extend RIPA interception powers by requiring foreign companies to comply both with section 8(1) interception warrants relating to named individuals or premises and section 8(4) 'external' interception warrants. Interception of 'external' communications – a communication either sent and/or received outside the British Islands – under section 8(4) is currently very loosely controlled. A section 8(4) warrant does not need to identify specific individuals or premises but need only contain descriptions of intercepted material. The security agencies currently interpret RIPA's 'external communication' powers to allow blanket interception and keyword processing; possibly even intercepting all communications emanating from or received in a particular country. We believe (particularly in light of Tempora reports) that external interception warrants may authorise the interception of 'all communications leaving the British Islands'. While the power to serve these warrants currently applies to providers within our jurisdiction, clause 4 purports to allow interception warrants to be served around the world. As a result of clause 4, the Secretary of State could serve Gmail with a section 8(4) warrant in California, USA, requiring it to intercept all communications between subscribers in two specified countries or, for example, all communications leaving or entering the UK.

25. External interception powers are currently subject to legal challenge by Liberty, Privacy International and others in the Investigatory Powers Tribunal (IPT) on the basis that they are so broad so as to allow blanket bulk interception of

communications. Clause 4 is likely to substantially increase the ability of GCHQ to acquire bulk intercepted data and amounts to an unexpected extension of powers that are already the subject of widespread public concern. Further, in extending the entire RIPA interception regime globally, the Bill appears to give the UK powers to require telecommunications service providers and internet services around the world to build interception capabilities into their products and infrastructure. We think the move to enact clause 4 could be in direct response to ongoing legal challenges to bulk interception and intended to provide an alternative route for the practice should the existing powers that are subject to challenge be found to breach Article 8 of the ECHR.

26. Clause 4 also purports to give extra territorial effect to communications data access requests. When the Draft Communications Data Bill (Snoopers' Charter) was published, a principle concern expressed by the Government was that much communications data was generated by service providers based in the US rather than those based in the UK. It argued that this led to a capability gap: the UK based companies subject to RIPA Part 1, Chapter 2, section 22(4) (requests to obtain or disclose communications data) were not retaining this information – the Government could not get it from overseas providers who were not subject to the UK's retention or acquisition regime. Why if the Government was so confident in its legal authority to require communications data from companies based overseas (as it now claims) did it seek to require domestic communication service providers to retain 'third party' communications data in the Draft Bill?

Clause 5: Meaning of "telecommunications service"

27. Clause 5 of the Bill significantly extends the scope and definition of "telecommunications service". The definition now includes any case where a service "*consists in or includes facilitating the creation, management or storage of communications transmitted or which may be transmitted*" which the explanatory notes explicitly state "*includes companies that provide internet based services such as webmail".*

28. This clause (read in conjunction with clause 4(8) gives new, express powers to go to foreign *internet based service providers* and demand that they hand over (or where they don't already have the information, obtain it then hand it over) communications data. The Government has claimed that nothing in the Bill creates

the powers sought under the Draft Communications Data Bill. However clause 4 goes a significant way to achieve data access previously sought via that Bill: namely communications data generated by 'third party' web service providers outside of the jurisdiction.

Conclusion

29. This fast track legislation contains sweeping surveillance powers that will affect every man, woman and child in the UK. The Bill contains the powers for Government to continue to mandate the blanket retention of the communications data of the whole population for 12 months. This is in direct contradiction of a Court judgment which held that blanket indiscriminate retention of communications data breached human rights. The Bill also contains new and unprecedented powers for the UK Government to require overseas companies to comply with interception warrants and communications data acquisition requests and mandate overseas companies to build interception capabilities in to their products and infrastructure. These provisions will expand interception powers currently being challenged in the British courts appearing to enable the Government to issue interception warrants mandating mass surveillance outside of the United Kingdom.

30. The two governing principles of our unconsolidated Constitution are parliamentary sovereignty and the Rule of Law. This Bill disrespects the first by containing a programme, agreed in secret between the three main party leaders over weeks of private meetings, denying the legislature time for scrutiny, amendment or even proper debate. The Bill shows utter contempt for the latter by attempting to overrule rather than comply with a Court judgment.

Isabella Sankey
Director of Policy