Data Retention And Investigatory Powers Bill

Human Rights Memorandum By The Home Office

1. This memorandum addresses issues arising under the European Convention on Human Rights ("ECHR") in relation to the Data Retention and Investigatory Powers Bill. The Department is satisfied that, in the event that the Bill is introduced into Parliament, the responsible Minister could make a statement under section 19(1)(a) of the Human Rights Act 1998 that, in his or her view, the provisions of the Bill are compatible with the Convention rights.

The Bill

2. The Bill makes provision for the retention of communications data by telecommunications service providers, replacing the regime contained in the Data Retention (EC Directive) Regulations 2009 ("the 2009 Regulations"). It also amends Chapter 1 of Part 1 of the Regulation of Investigatory Powers Act 2000 ("RIPA") to clarify that certain powers in respect of the interception of communications are exercisable in relation to providers located outside the UK.

3. Clause 1(1) of the Bill contains measures enabling the Secretary of State, by notice, to require providers of telecommunications services to retain certain types of communications data generated or processed by them in the course of supplying their services. The types of data to be retained are those set out in the Schedule to the 2009 Regulations. A notice may require the retention of data for a period of up to 12 months. Clause 1(3) contains a regulation-making power to make further provision about the retention of such data, including, for example, by setting out further details of the data to be retained and to impose safeguards relating to the security of, access to and destruction of the retained data. Retained data must only be disclosed in accordance with the procedures under Chapter 2 of Part 1 of RIPA, or court order.

4. Clause 3 amends RIPA so that a warrant may only be issued, or a notice or authorisation for access to communications data given, on the ground that it is necessary for the purpose of safeguarding the economic well-being of the UK where that purpose is linked to national security. That is already the position taken in practice, and is reflected in statutory codes of practice under section 71 of RIPA.

5. Clause 4 makes provision to clarify that the power to serve an interception warrant on a person who may provide assistance in giving effect to the warrant[1] may be exercised in respect of a person outside the UK. Similarly, the power of the Secretary of State to give a notice requiring a public telecommunications service provider to maintain a permanent interception capability[2] may be exercised in respect of a public telecommunications provider outside the UK. Similar provision is made in respect of obtaining communications data from

[1] Section 11(2) of RIPA.
[2] Section 12(1) of RIPA; The Regulation of Investigatory powers (Maintenance of Interception Capability) Order 2002 (S.I. 1931/2002).

providers. Further amendments make provision in respect of the practicalities of service on, or giving a notice to, such a provider. In clause 5, the definition of 'telecommunications service' is clarified to make explicit that the term 'telecommunications service provider' is intended to capture those providers whose services are internet-based (such as web-based email) as well as those providing infrastructure for connection to the internet.

Background

6. Communications data is the context not the content of a communication. It can be used to demonstrate who was communicating; when; from where; and with whom. It can include the time and duration of a communication, the number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It does not include the content of any communication: for example the text of an email or a conversation on a telephone.

7. Communications data is used by the intelligence and law enforcement agencies during investigations regarding national security, as well as serious and organised crime. It enables investigators to identify members of a criminal network, place them in specific locations at given times and in certain cases to understand the criminality in which they are engaged. Communications data can be vital in a wide range of threat to life investigations, including the investigation of missing persons. Communications data can be used as evidence in court.

8. Communications data is retained in the UK primarily in reliance on the 2009 Regulations. Those regulations implement the UK's obligations under the Data Retention Directive (2006/24/EC) ("the Directive"), which has been ruled invalid by the ECJ. The 2009 Regulations were made in reliance on the power in section 2(2) of the European Communities Act 1972.

9. On 8 April 2014, the Grand Chamber of the European Court of Justice gave judgment in two joined preliminary references[3] on the validity of the Data Retention Directive. The Court ruled that the Directive is invalid on the grounds that it breached Articles 7 and 8 of the EU Charter of Fundamental Rights (the right to respect for family and private life, and the right to protection of personal data).

10. The Court accepted that the objective of the Directive, to contribute to the fight against terrorism and serious crime, and to maintain public security, is a legitimate justification for interfering with the rights in question. However, the Court found that the extent of that interference was disproportionate. The rights in question were important and the interference with those rights was very serious. The Court found that the conditions under which data could be retained should have been more closely defined in the Directive.

11. The Court listed a range of conditions and safeguards which were not included in the Directive. In the absence of any of those conditions, it found that the retention

[3] C-293/12 Digital Rights Ireland & C-594/12 Seitlinger.

of data in accordance with the Directive was a disproportionate interference with the fundamental rights in question, and the Directive is accordingly invalid. In particular, the European Court of Justice found that the Directive did not contain:

a. Any restrictions on the types of data retained – the Directive covered all persons, all means of electronic communications and all traffic data;
b. Any conditions limiting the categories of data that is retained – for example limitations by geographical location, or by link to serious crime. Nor was it limited by category of person, so for example records of lawyers' communications and other privileged information would be retained;
c. Any objective criteria on access to data and their subsequent use, simply referring to 'serious crime' as defined by Member States, and did not restrict access to the purpose of preventing / detecting serious crime;
d. Any requirement of prior review by a court or independent administrative body to determine the necessity of the request for the purposes of preventing or detecting serious crime;
e. Any different retention periods for different types of traffic data, or any requirement that the retention period be based on objective criteria;
f. Sufficient safeguards for the protection of data, having regard to the quantity of data retained, the sensitive nature of the data, and the risk of unlawful access to the data. In particular, the Directive allowed CSPs to have regard to economic considerations when determining the level of security applied, and did not require irreversible destruction at the end of the period of retention.

12. The Directive was aimed at harmonising measures for the retention of communications data across the EU, and was never intended to contain a comprehensive system of safeguards or details of the access regime, which were intended to be matters for Member States. Accordingly, the 2009 Regulations deal primarily with the retention of data, while detailed provision for access to the retained communications data is set out in Chapter 2 of Part 1 of RIPA, and the Regulation of Investigatory Powers (Communications Data) Order 2010 (SI 2010/480) made under it. Both contain stringent safeguards on access to data.

13. As well as the 2009 Regulations, some data is retained by telecommunications providers on the basis of the voluntary code of practice under Part 11 of the Anti-terrorism Crime and Security Act 2001. Data retained by providers is subject to the safeguards contained in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), and in the Data Protection Act 1998.

14. The Department's position is that the existing safeguards in domestic legislation concerning the security of retained data and restrictions on access to that data are sufficient to meet the concerns set out in the ECJ judgment. Nevertheless the provisions in the Bill seek to include further safeguards in relation to the security of, and access to, that retained data to strengthen the position.

Interception of communications

15. The interception of communications in the course of their transmission in the UK is governed by the Regulation of Investigatory Powers Act 2000, designed to be

an ECHR-compliant scheme. The proposed amendments to Chapter 1 of Part 1 of the Act do not seek to extend the scope of the existing powers or provisions of that Chapter, but simply to clarify that it may have extra-territorial effect in certain circumstances, and to clarify the services which are captured by the definition of a 'public telecommunications service'.

Article 8

Generally

16. It is established that mail, telephone and email communications are covered by the notion of private life and correspondence in Article 8(1). There is a series of cases to the effect that interception of the content of communications is an interference with those rights. There is limited Strasbourg case law on the application of Article 8 to communications data, but the case of *Malone v UK* (1984) 7 EHRR 14 (paragraphs 83 to 88) provides some limited guidance, to the effect that while it is to be distinguished from the interception of the content of communications, Article 8 issues still arise. In that case, the release of telephone metering information to the police constituted an interference with an Article 8 right.

17. Article 8 may also impose positive obligations on States to adopt measures designed to secure respect for private life between private persons. It follows that there may be a breach of such positive obligations if the State requires private persons to interfere excessively with the privacy of others, or in the absence of adequate safeguards[4].

18. Clause 1 of the Bill will enable the Secretary of State to impose requirements and restrictions on telecommunications operators to retain communications data. Article 8 imposes positive obligations upon the State as a whole to regulate the performance of the duties imposed on operators under clause 1 and, in particular, to ensure that there are appropriate safeguards in place. The requirement to retain data must be assessed together with all other relevant measures that are in place to respect and protect privacy[5].

19. The amendments to Chapter 1 of Part 1 of RIPA are merely clarificatory, and will not result in any additional interference with Art 8(1) rights. The powers of the Secretary of State to authorise the interception of communications are not broadened by the Bill.

Article 8(2)

20. Article 8(2) sets out the grounds on which interferences with the protected rights may be justified. Justification of an interference under Article 8(2) requires that

[4] See e.g., *Botta v Italy* (1998) 26 EHRR 241, at para. 33.
[5] See *Von Hannover v. Germany* (2004) 40 EHRR 1.

the interference in question is: (i) "in accordance with the law", (ii) for a legitimate aim (or aims) and (iii) proportionate, having regard to the aim (or aims) at issue.

Communications data

21. The interferences will be in accordance with the law because there will be clear provision in legislation governing the requirement on operators to retain communications data (i.e. in the new legislation), and the circumstances in which the communications data may be obtained by relevant public authorities (i.e. in Chapter 2 of Part 1 of RIPA, to which there is an explicit link in the Bill). These provisions are formulated with sufficient precision to enable a person to know in what circumstances and to what extent the powers can be exercised. It is the Department's position that the relevant test of foreseeability in the context of the retention of and access to communications data is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. The provisions of the Bill and regulations to be made under it, together with the provisions of Chapter 2 of Part 1 of RIPA, meet that test.

22. The interferences with Convention rights will be in pursuit of a legitimate aim. The ability of law enforcement and intelligence agencies to obtain communications data is vital in protecting national security, preventing and detecting crime and protecting the public[6]. Communications data is used not only as evidence in court, but also to eliminate people from law enforcement investigations. It can be used to prove a person's innocence as well as his or her guilt. It is essential that communications data of this sort continues to be available to be obtained by the law enforcement and intelligence agencies and other relevant public authorities. The ECJ judgment in Digital Rights Ireland recognises that data relating to the use of electronic communications 'are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime' and concluded that their retention genuinely satisfies an objective of general interest.

23. A notice imposing a requirement on a provider to retain data may only be given if the Secretary of State believes that it is necessary and proportionate to do so for one or more of the legitimate aims set out in section 22(2) of RIPA:

    a. in the interest of national security,
    b. for the purpose of preventing or detecting crime or of preventing disorder,
    c. in the interests of the economic well-being of the United Kingdom,
    d. in the interests of public safety,
    e. for the purpose of protecting public health,

[6] See e.g., K.U. v Finland [2008] ECHR 2872/02, at para. 49 ("....Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. …It is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context."

f. for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
g. for the purpose, in an emergency, of preventing death or injury 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,
h. to assist investigations into alleged miscarriages of justice[7], or
i. where a person ("P") has died or is unable to identify themselves because of a physical or mental condition-
    i. to assist in identifying P, or
    ii. to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

24. The interferences with these rights will also be proportionate for the reasons set out below, including the extensive range of safeguards and restrictions against abuse. The safeguards in relation to the data which must be retained are as follows.

25. The Bill limits the circumstances in which providers may be required to retain data, and the data they may be required to retain. The categories of data that are to be retained are limited to those set out in the Schedule to the 2009 Regulations. This is by no means all the communications data that may exist in relation to an individual's communications. The notice-giving power in clause 1 enables the Secretary of State to limit the requirement to retain to a description of data held by a provider, so a notice need not require the retention of all data by a particular operator (but may extend to all relevant data if that requirement is necessary and proportionate).

26. The requirement to retain data may be for a maximum period to be provided for in regulations, but of no more than 12 months. A notice may impose different requirements in respect of different types of data, so, for example, a shorter retention period could be specified in respect of a certain category of data. The requirements of a notice will be tailored according the assessment of the necessity and proportionality of retention. Regulations will provide that a notice must be kept under review.

27. In practice, it is likely that a notice requiring the retention of data will provide for more specific requirements or restrictions relating to particular systems and services provided by an operator, and will impose requirements with respect to particular descriptions of data.

28. The Bill also provides for the introduction of an extensive range of safeguards against abuse of retained data to ensure that operators are subject to all the obligations necessary to secure respect for the private life of individual telecommunications users. The relevant safeguards will be set out in secondary legislation made under clause 1(3). Draft regulations will be made available to Parliament during the passage of the Bill. The safeguards will include: a requirement to secure the integrity of retained data and subject it to the same

[7] Purposes h and i are contained in the Regulation of Investigatory Powers (Regulation of Investigatory Powers (Communications Data) Order 2010 (S.I. 2010/480).

security and protections as the data on the operator's systems; a requirement to secure, by organisational and technical means, that data can only be accessed by specially authorised personnel; and a requirement to protect the retained data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure. The retained data must be destroyed by the operator if the retention of the data ceases to be authorised (if, for example, a notice under clause 1 is revoked, or at the end of the retention period specified in the notice). Data must be deleted in such a way as to make access to the data impossible.

29. The Regulations will also provide for the Information Commissioner to audit compliance by providers with the requirements in respect of the retention of data.

30. There will be safeguards in place to ensure that access to the retained data by public authorities is only available in defined circumstances. Clause 1(6) provides that operators may only disclose retained data in accordance with the scheme under Chapter 2 of Part 1 of RIPA, which provides guarantees against abuse, or in accordance with a court order or warrant (or other circumstances approved by Parliament in the Regulations).

31. Under section 22 of RIPA access is only permitted by authorised public authorities. Public authorities are authorised to access different categories of data for different purposes. A notice or authorisation to access communications data must be necessary and proportionate for one of the authorised purposes, taking into account any collateral intrusion.

32. Section 57(2) of RIPA provides for the independent Interception of Communications Commissioner to keep under review the exercise of powers and duties under Chapter 2 of Part 1. The Commissioner must have previously held high judicial office. His inspection team actively examine applications to ensure the decision making (around necessity and proportionality) is appropriately rigorous.

33. The Commissioner publishes a report annually which outlines where mistakes have been made in the application process, as well as outlining full statistics for all public authorities who have used their powers. If the Commissioner becomes aware of any circumstance in which an error is wilful or reckless, he can inform the person to whom the error relates to enable them to make a complaint to the Independent Investigatory Powers Tribunal.

34. If any person believes their data has been acquired inappropriately they can complain to the independent Investigatory Powers Tribunal, which can investigate the details of the case, and order compensation.

35. The Home Office accordingly considers that interferences with the Article 8(1) rights will be proportionate.

36. The European Court of Human Rights has accepted that States should be accorded a wide margin of appreciation in this area (see *Weber and Saravia v. Germany* (2008) 46 EHRR SE5, at paragraph 106), and some limited support can

be derived from *Malone* for the proposition that the Court considers the acquisition of communications data to be a less serious infringement of privacy rights than the interception of communications

37. It is essential that the UK is able to obtain communications data in the interests of national security and the prevention and detection of crime. The reduction in the availability of communications data would have extremely serious consequences for the UK. The provisions in the Bill are an essential measure to ensure a firm legal basis for the retention of communications data, to ensure that public authorities continue to have sufficient access to communications data to perform their duties and to support intelligence agency and law enforcement activities.

33. The Bill, together with existing domestic legislation, addresses the majority of the criticisms of the Directive set out in the ECJ's judgment.

Interception

33. The interferences involved in activities under Chapter 1 of Part 1 of RIPA are in accordance with the law. There is clear provision in legislation providing a basis for interception. RIPA, and the Statutory Code of Practice on Interception made under it, are compatible with the rule of law and accessible. In the context of interception of communications, the Strasbourg Court has ruled that foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (*Leander v Sweden*), but the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to intercept communications. The law must indicate the scope of the competent authorities' discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

34. The Strasbourg Court has developed a set of 'minimum safeguards' that need to be set out in the domestic legal framework that governs the interception of communications, in order to ensure that the foreseeability requirement is met. Those minimum safeguards, as set out in the *Weber and Saravia* case, are:
    a. The nature of the offences which may give rise to an interception order;
    b. A definition of the categories of people liable to have their telephones tapped;
    c. A limit on the duration of telephone tapping;
    d. The procedure to be followed for examining, using and storing the data obtained;
    e. The precautions to be taken when communicating the data to other parties; and
    f. The circumstances in which recordings may or must be erased or the tapes destroyed.

35. In *Kennedy*, the Court found that the law governing the interception of communications between persons in the United Kingdom (which may be made by means of a telecommunications service provided by a person located outside the UK) was sufficiently foreseeable.

36. The *Liberty v UK* case concerned the interception of communications between the UK and any other country. The Court in that case considered that the law in force at the relevant time, the Interception of Communications Act 1985, was not sufficiently foreseeable since it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material, in the context of the interception of communications at issue in that case. The 1985 Act did not have an accompanying Code of Practice. The Home Office's position is that RIPA, which replaced the 1985 Act, and its accompanying Code of Practice on the Interception of Communications, made under section 71 of RIPA, satisfy the 'in accordance with law' requirement in respect of the interception of external communications.

37. The Bill arguably increases the foreseeability of the powers in Chapter 1 of Part 1 of RIPA by making clearer that assistance with the implementation of interception warrants may be effected outside the jurisdiction, and by clarifying the services which are captured by the definition of 'telecommunications service'. But it is the Department's position that the interferences in question are in accordance with the law on the basis of the current legislation.

38. The interferences with Convention rights are in pursuit of a legitimate aim. The ability of law enforcement and intelligence agencies to intercept communications is vital in protecting national security and preventing and detecting crime. A warrant authorising the interception of communications may only be granted by the Secretary of State where she considers it necessary in the interests of national security, for the prevention or detection of serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom (which will be expressly limited by clause 3 of the Bill to circumstances where there is a link to national security), and proportionate to what is sought to be achieved.

39. The interferences will also be proportionate. RIPA and the Code of Practice contain a range of safeguards around the interception of communications, and the processing and communication of intercepted material.

40. Accordingly, the Department considers the Bill is compatible with Article 8.

Article 1 of Protocol 1

41. The imposition of requirements upon telecommunications operators under the Bill may give rise to interferences with their rights under Article 1 of Protocol 1. Operators may incur costs in complying with obligations under the Bill, which could constitute an interference with their peaceful enjoyment of their possessions, in the form of their business interests.

42. Article 1 of Protocol 1 is a qualified right. The imposition of requirements on telecommunications operators will be in accordance with the law because they will be contained in primary legislation and are formulated with sufficient precision to enable a person to know in what circumstance they can be exercised. The

requirements will be in the general interest because they will secure the availability of communications data which is essential to the law enforcement intelligence agencies in protecting national security, preventing and detecting crime and protecting the public. The requirements will be proportionate for the reasons set out above and because the expectation is that most of the operators' costs of complying with any new obligations in the Bill will be met from public funds (i.e. so as to ensure that the operators will in effect receive 'compensation' for any interferences with their rights under Article 1 of Protocol 1).

43. Accordingly, the Department considers the Bill is compatible with Article 1 of Protocol 1.

Home Office
11 July 2014