These notes refer to the Data Retention and Investigatory Powers Act 2014 (c.27) which received Royal Assent on Thursday 17 July 2014

DATA RETENTION AND INVESTIGATORY POWERS ACT 2014

EXPLANATORY NOTES

BACKGROUND

Retention of communications data

8. 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. Communications data is used by the intelligence and law enforcement agencies during investigations regarding national security and organised and serious 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.

9. Telecommunications companies retain communications data for a number of reasons: for business purposes; through voluntary agreement with the Government or through mandatory requirements. Mandatory retention is covered by the 2009 Regulations, which provide for telecommunications companies that have been issued a notice by the Secretary of State to retain the data types specified in the Schedule to the Regulations for a period of 12 months. Part 11 of the Anti-terrorism, Crime and Security Act 2001 provides for data retention through a voluntary code. Under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), companies are permitted to retain data they need for business purposes. However, once the data is no longer needed for those purposes it must be deleted or made anonymous, unless otherwise required by law.

10. Without mandatory data retention, relevant public authorities would still be able to access data retained under the voluntary code or for business purposes. However, this is not a substitute for the 2009 Regulations. Many companies are not signed up to the voluntary code and certain types of data may only be retained for a matter of days. Much of the data retained for business purposes would be deleted after only a few months, rather than the 12 months required by the 2009 Regulations. A 2012 Association of Chief Police Officers survey demonstrated that many investigations require data that is older than the few months that data may be retained for business purposes, particularly in ongoing investigations into offences such as child abuse and financial crime.

11. On 8 April 2014 the ECJ gave a judgment declaring the Data Retention Directive to be invalid. The Data Retention (EC Directive) Regulations 2007 (S.I. 2007/2199) implemented the Directive in respect of mobile and fixed line telephony. The 2009 Regulations, which revoked and replaced the 2007 Regulations, implemented the

Directive with respect to the retention of communications data relating to internet access, internet telephony and internet e-mail as well as mobile and fixed line telephony.

12. This Act provides powers to replace the 2009 Regulations. 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 United Kingdom's comprehensive data retention and access regime. Nevertheless, where appropriate, the Act adds safeguards while providing for the replacement regulations to add further safeguards in line with the judgment.

13. Specifically, the Act provides a power for the Secretary of State to issue a data retention notice on a telecommunications services provider, requiring them to retain certain data types. The data types are those set out in the Schedule to the 2009 Regulations. No additional categories of data can be retained. The Act provides that the period for which data can be retained can be set at a maximum period not to exceed 12 months, rather than the fixed 12 months in the 2009 Regulations, allowing for retention for shorter periods when appropriate. It provides a power to make regulations setting out further provision on the giving of and contents of notices, safeguards for retained data, enforcement of requirements relating to retained data and the creation of a code of practice in order to provide detailed guidelines for data retention and information about the application of safeguards. The regulations may also provide for the revocation of the 2009 Regulations, and transitional provisions.

The Regulation of Investigatory Powers Act 2000

14. Chapter 2 of Part 1 of RIPA provides a regulatory framework for the acquisition of communications data. For example, necessity and proportionality tests are carried out by a designated senior officer, at a rank stipulated by Parliament, within a public authority before a request for data can be made. Section 25(1) of RIPA defines what constitutes a relevant public authority. Section 22(2) of RIPA provides the purposes for which communications data may be accessed. The Secretary of State has powers to add or remove public authorities and add purposes through secondary legislation.

15. Regarding interception, Chapter 1 of Part 1 of RIPA allows for law enforcement and security and intelligence agencies to gain access to the content of communications made by post or telecommunications. There are a number of safeguards. For example, access is only permitted under warrant from the Secretary of State. The Secretary of State must be satisfied that the interception is necessary for the purposes of national security, the prevention or detection of serious crime, or the economic well-being of the United Kingdom (where this specifically relates to national security), and proportionate to what is sought to be achieved. The information must not be able to be reasonably obtained by other means.

16. In part, this Act was required in order to clarify the intent of RIPA. While RIPA has always had implicit extraterritorial effect, some companies based outside the United Kingdom, including some of the largest communications providers in the market, had questioned whether RIPA applies to them. These companies argue that they will only comply with requests where there is a clear obligation in law. When RIPA was drafted it was intended to apply to telecommunications companies offering services to United Kingdom customers, wherever those companies were based.

17. The Act therefore clarifies the extra-territorial reach of RIPA in relation to both interception and communications data by adding specific provisions. This confirms that requests for interception and communications data to overseas companies that are providing communications services within the United Kingdom are subject to the legislation.

18. The Interception of Communications and the Acquisition and Disclosure of Communications Data codes of practice, made under section 71 of RIPA, specify that interception warrants can only be issued and communications data can only be obtained

on the grounds of economic well-being when specifically related to national security. This Act makes this clear in primary legislation.

19. The Act also amends the definition of "telecommunications service" in RIPA. This is for the purposes of communications data and interception requests. It confirms that the full range of services provided by domestic and overseas companies to customers in the United Kingdom is covered by the definition.

Review of Investigatory Powers and Commissioner's Reports

20. There are already oversight and review arrangements for investigatory powers in existing legislation. Nevertheless, this Act goes further. Section 36(1) of the Terrorism Act 2006 provides for the appointment of an independent reviewer of terrorism legislation ("the independent reviewer"), currently David Anderson Q.C. This Act requires the Secretary of State to commission from the independent reviewer a review of the investigatory powers available in the United Kingdom and how they are regulated. The review will therefore include the contents of this Act and any regulations made under it. The independent reviewer should report before 1 May 2015.

21. Sections 57 and 58 of RIPA provide for the appointment of an Interception of Communications Commissioner to carry out a yearly report. The Commissioner is currently the Rt Hon. Sir Anthony May. His remit includes reviewing the Secretary of State's role in issuing interception warrants and the operation of the regime for the acquisition of communications data. This Act ensures that the Commissioner will be required to report twice a year on these issues.