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

INTRODUCTION

1. These explanatory notes relate to the Data Retention and Investigatory Powers Act 2014 which received Royal Assent on Thursday 17 July 2014. They have been prepared by the Home Office in order to assist the reader of the Act and to help inform debate on it. They do not form part of the Act and have not been endorsed by Parliament.

2. The notes need to be read in conjunction with the Act. They are not, and are not meant to be, a comprehensive description of the Act. So where a section or part of a section does not seem to require any explanation or comment, none is given.

SUMMARY

3. The Government decided to legislate in order to clarify the legislative framework for certain important investigatory powers. Firstly, this Act provides the powers to introduce secondary legislation to replace the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859) ("the 2009 Regulations"), while providing additional safeguards. This is in response to the European Court of Justice ("ECJ") judgment of 8 April 2014 in joined cases C-293/12 Digital Rights Ireland & C-594/12 Seitlinger which declared the Data Retention Directive (2006/24/EC) invalid. The 2009 Regulations implemented the Directive in domestic law. Secondly, the legislation clarifies the nature and extent of obligations that can be imposed on telecommunications service providers based outside the United Kingdom under Part 1 of the Regulation of Investigatory Powers Act 2000 ("RIPA"). This Act ensures that, as the original legislation intended, any company providing communication services to customers in the United Kingdom is obliged to comply with requests for communications data and interception warrants issued by the Secretary of State, irrespective of the location of the company providing the service. Both these components of the Act strengthen and clarify, rather than extend, the current legislative framework. Neither of these components provide for additional investigatory powers. The Act also provides for a review of the operation and regulation of investigatory powers in relation to communications data and interception and increased reporting from the Interception of Communications Commissioner.

4. The first component of the Act relates to Government requirements for retention of communications data. Mandatory data retention is necessary because without it data protection law requires service providers to delete data that they no longer need for business purposes. Mandated data retention is crucial for law enforcement to investigate, detect and prevent crimes. Ensuring certain types of communications data are retained provides the confidence that the data required will be available when needed by public bodies that have been approved by Parliament to acquire it. Its acquisition is strictly controlled by RIPA.

5. The second element of the Act puts beyond doubt that the interception and communications data provisions in RIPA have extra-territorial effect. Interception

provides, under strict conditions and for a limited number of public authorities, access to the content of a communication. This Act does not alter the existing safeguards which regulate interception. Law enforcement and intelligence agencies will continue to require an interception warrant signed by the Secretary of State. The Act also clarifies the economic well-being purpose for obtaining communications data or issuing an interception warrant under RIPA, and the definition of a "telecommunications service". This is to ensure 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. Clarifying the definition of "telecommunications service" ensures internet-based services, such as webmail, are included in the definition.

6. The third element of the Act provides for a review of investigatory powers to report by 1 May 2015. It also provides for more frequent reporting from the Interception of Communications Commissioner.

7. Statutory arrangements in relation to communications data and intercept have been in place for a number of years. However, in response to recent developments, the Government considered it important to legislate in order to put beyond any legal doubt the regime for both investigatory techniques.

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.

OVERVIEW

22. The Act provides powers to create a new mandatory data retention regime to replace the 2009 Regulations.

23. It clarifies that the economic well-being purpose for obtaining communications data or issuing an interception warrant under RIPA must relate to national security.

24. It clarifies the extra-territorial reach of RIPA for the purposes of seeking assistance with giving effect to an interception warrant, giving a notice requiring the maintenance of a permanent interception capability, or requesting communications data.

25. It provides further clarification of the detail of the definition of a telecommunications service.

26. Finally, it provides for the review of the investigatory powers available in the United Kingdom and increased reporting on their use.

TERRITORIAL EXTENT AND APPLICATION

27. The Act extends to the whole of the United Kingdom. In relation to Scotland, Wales and Northern Ireland the provisions relate to reserved matters.

COMMENTARY

Retention of relevant communications data

Section 1: Powers for retention of relevant communications data subject to safeguards

28. *Subsection (1)* replaces provisions in the 2009 Regulations to allow the Secretary of State to give a notice to a telecommunications service provider requiring the retention

of data. The notice may require the retention of 'relevant communications data', defined in section 2(1) as the data types set out in the Schedule to the 2009 Regulations. The Schedule includes data falling into the categories of fixed network telephony (part 1), mobile telephony (part 2), and internet access, internet e-mail or internet telephony (part 3). Section 1 creates the additional safeguard that the Secretary of State must consider whether it is necessary and proportionate to give the notice for one or more of the purposes set out in section 22(2) of RIPA. These purposes, which are the same purposes for which retained data can be accessed under RIPA, are:

a) in the interests 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;

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; or

h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of section 22(2) by an order made by the Secretary of State.

29. The economic well-being purpose for which communications data may be accessed is amended in section 3 of the Act and this change feeds through into the corresponding purpose for the retention of relevant communications data.

30. The Secretary of State has previously added the following further purposes:

a. to assist investigations into alleged miscarriages of justice, or

b. 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.

31. Telecommunications service providers will not be required to retain data unless they have been given a notice by the Secretary of State.

32. *Subsection (2)* lists the issues a notice may cover. Paragraph (a) specifies that the notice can apply to a specific telecommunications service provider. Alternatively, it can provide a description of providers to ensure that all those that fit the description are required to retain data. Paragraph (b) provides that a notice may require the retention of all data or any description of data. A notice cannot require the retention of data types other than those that were required to be retained by the 2009 Regulations, but may limit the requirement to a subset of these data types where appropriate. Paragraph (c) allows for a retention notice to specify the period or periods for which data is to be retained. Paragraph (d) provides for a notice to include requirements and restrictions in relation to data retention. Therefore, for example, a notice could require a provider to keep data retained under a notice in a separate store from data retained for other purposes. Paragraph (e) allows for a notice to make different data types subject to different provisions so, for example, there may be a requirement to retain different types of data for different periods of time. Paragraph (f) permits the data retention notice to apply to data whether or not the data is in existence at the time of the notice. If the

data is in existence the maximum amount of time new regulations would permit it to be retained will still be 12 months (see subsection (5)).

33. *Subsection (3)* allows for the Secretary of State to make regulations relating to the retention of relevant communications data. These regulations will replace the 2009 Regulations.

34. *Subsection (4)* gives examples of the matters that may be provided for in the regulations. This includes: what the Secretary of State should consider before issuing a notice; the procedure for when the notice will come into force, including variation or revocation; the integrity and security of the retained data; enforcement and auditing compliance; a code of practice which will provide specific guidelines on data retention; the reimbursement of telecommunications service providers who incur costs while fulfilling any obligations in their notice; and the transitional measures from the 2009 Regulations.

35. *Subsection (5)* specifies that the maximum retention period which can be provided for in the regulations made under subsection (3) is 12 months from a date specified in the regulations.

36. *Subsection (6)* specifies that data retained under the provisions in this legislation can only be acquired through Chapter 2 of Part 1 of RIPA, through an order of the court or other judicial warrant or authorisation, or as specified in regulations made under subsection (3).

37. *Subsection (7)* permits the Secretary of State to make regulations which apply any provision that is capable of being made by virtue of subsections (4)(d) to (4)(g) or subsection (6) to data that is retained on a voluntary basis under the Anti-terrorism, Crime and Security Act 2001 ("ATCSA"). This power could be used to apply the safeguards in the regulations to data retained under the ATCSA.

Section 2: Section 1: supplementary

38. *Subsection (1)* provides relevant definitions. The Act uses definitions of telecommunications service provider and communications data as set out in Part 1 of RIPA. This is to ensure uniform definitions across access and retention regimes. Other definitions of terms used in the list of categories of data remain as set out in the 2009 Regulations. 'Relevant communications data' is defined as the data mentioned in the Schedule to the 2009 Regulations, so far as that data is generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned. The definition of public telecommunications operator ensures that a telecommunications systems provider or a telecommunications service provider can be subject to a notice. This distinction occurs, for example, when a company uses the physical network (this includes the network bandwidth and phone lines) belonging to another in order to provide their services to the public. The definition ensures that a request to retain can be imposed on whichever company holds the relevant data (which will depend on how they design their systems).

39. *Subsection (2)* provides that 'relevant communications data' includes data relating to unsuccessful call attempts but not unconnected calls. An unsuccessful call occurs, for example, when the person being dialled does not answer the call, but where the network has been able to successfully connect it. An unconnected call is where, for example, a call is placed, but the network is unable to carry it to its intended recipient. It is also made clear that "relevant communications data" is not the content of the communication.

40. *Subsection (3)* provides for the regulations to replicate the Schedule to the 2009 Regulations, for ease of reference and so the position is clear once the 2009 Regulations have been revoked.

41. *Subsection (4)* provides for the regulations under section 1 to be made by statutory instrument and for such regulations, by virtue of subsection (4)(b)(i), to confer or impose functions on any person. Paragraph (c) allows for codes of practice to be made, in particular by modifying sections 71 and 72 of RIPA.

42. *Subsection (5)* specifies that any statutory instrument under section 1 will be subject to the affirmative resolution procedure.

Investigatory powers

Section 3: Grounds for issuing warrants and obtaining data

43. *Subsections (1)* and *(2)* amend section 5 of RIPA regarding the Secretary of State's power to issue interception warrants on the grounds of economic well-being. The Interception of Communications Code of Practice, made under section 71 of RIPA, specifies that interception warrants can only be issued on such grounds when economic well-being is directly related to national security. In the interests of clarity, the Act makes express provision for this requirement by amending RIPA.

44. *Subsections (3)* and *(4)* make the same amendment as subsections (1) and (2) but with respect to access to communications data. The Acquisition and Disclosure of Communications Data Code of Practice, made under section 71 of RIPA, specifies that data can only be acquired in the interests of the economic well-being of the United Kingdom when it specifically relates to national security. The Act also makes express provision for this requirement by amending RIPA.

Section 4: Extra-territoriality in Part 1 of RIPA

45. This section clarifies certain provisions of Chapters 1 and 2 of Part 1 of RIPA to put beyond doubt that those provisions have extra-territorial effect.

46. *Subsection (1)* provides that Part 1 of RIPA is amended.

47. *Subsection (2)* inserts new subsections into section 11 of RIPA (implementation of interception warrants). New subsection (2A) provides that a copy of an interception warrant may be served on a person outside the United Kingdom, and may relate to conduct outside the United Kingdom. New subsection (2B) provides for the practicalities of serving the warrant on a person based outside the United Kingdom. The warrant can be served (in addition to service by electronic or other means) at an office within the United Kingdom, to an address, specified by the overseas person, within the United Kingdom, or by making it available for inspection within the United Kingdom. New subsection (2C) provides that the method of service by making available for inspection is only available where no other means of service is reasonably practicable, and that appropriate steps must be taken to bring the warrant to the attention of the person on whom a copy is served.

48. *Subsection (3)* amends section 11(4) of RIPA. That subsection provides that where a copy of a warrant is served on a person who provides a postal service, a person who provides a public telecommunications service (defined as a telecommunications service provided to the public in the United Kingdom), or a person having control of telecommunication system in the United Kingdom, that person has a duty to take steps to give effect to the warrant. Subsection (3) amends section 11(4) to make clear the duty applies whether or not the person is in the United Kingdom.

49. *Subsection (4)* inserts a new subsection (5A) into section 11 of RIPA, which sets out factors to be taken into account when determining whether steps for giving effect to a warrant are reasonably practicable.

50. *Subsection (5)* amends section 11(8) of RIPA, which provides that the obligation to give effect to the warrant is enforceable by civil proceedings. The amendment clarifies that this applies where the person subject to the duty is outside the United Kingdom.

51. *Subsection (6)* inserts new subsections into section 12 of RIPA (maintenance of interception capability). New subsection (3A) specifies that the Secretary of State's power to give a notice requiring the maintenance of a permanent interception capability to a telecommunications service provider may be exercised in respect of a provider based outside the United Kingdom or in relation to conduct outside the United Kingdom. A public telecommunications service is one provided to the public in the United Kingdom. New subsection (3B) provides for the practicalities of giving a notice to a person based outside the United Kingdom. In addition to electronic or other means, it may be given by delivering it to an office in the United Kingdom, or to a specified address in the United Kingdom.

52. *Subsection (7)* amends section 12(7) of RIPA, which provides that where a notice to maintain an interception capability has been served on a telecommunications service provider, that person has a duty to comply with the notice, enforceable by civil proceedings for an injunction. The amendment makes clear that the duty, and the power to enforce, apply whether or not the telecommunications service provider is in the United Kingdom.

53. *Subsection (8)* inserts new subsections into section 22 of RIPA (obtaining and disclosing communications data). New subsection (5A) provides that an authorisation or a notice for the obtaining of communications data under section 22 may relate to conduct outside the United Kingdom, and a notice may be given to a person outside the United Kingdom. New subsection (5B) provides for the practicalities of giving a notice to a person outside the United Kingdom.

54. *Subsection (9)* amends section 22(6) of RIPA to make clear that the duty on a postal or telecommunications operator to comply with a notice applies whether or not the operator is in the United Kingdom.

55. *Subsection (10)* amends section 22(8) of RIPA to make clear that the power to enforce that duty by civil proceedings applies in respect of a person outside the United Kingdom.

Section 5: Meaning of "telecommunications service"

56. This section inserts a new subsection into section 2 of RIPA. New section 2(8A) makes clear that the definition of "telecommunications service" includes companies who provide internet-based services, such as webmail.

Section 6: Half yearly reports by the Interception of Communications Commissioner

57. RIPA provides for annual reports by the Interception of Communications Commissioner. This section amends RIPA to require the Commissioner to report half-yearly. As with the yearly reports, the half-yearly report must be laid before Parliament and sent to the Prime Minister. As in section 58(7) of RIPA, the Prime Minister will retain the power to exclude information from half-yearly reports. This includes when disclosure is against the public interest or for reasons of national security.

Section 7: Review of investigatory powers and their regulation

58. *Subsection (1)* provides for the Secretary of State to appoint the independent reviewer of terrorism legislation to review the regulation and operation of investigatory powers. The independent reviewer is a post that already exists under the Terrorism Act 2006. This section will add these additional responsibilities to his remit until a report has been provided to the Prime Minister (see subsection (4)).

59. *Subsection (2)* provides for the issues that the independent reviewer must consider. Specifically, the independent reviewer must consider current and future threats to the United Kingdom; capabilities needed to combat such threats; privacy safeguards; challenges faced by changing technologies; transparency and oversight; and the

effectiveness of existing legislation and whether there is a case for new or amending legislation.

60. *Subsection (3)* ensures, if reasonably practicable, that the review will be completed by 1 May 2015.

61. *Subsection (4)* specifies that a report on the outcome of the review must be sent to the Prime Minister.

62. *Subsections (5)* and *(6)* provide for the Prime Minister to lay a copy of the report before Parliament. If the Prime Minister decides that publishing certain sections of the report will be contrary to the public interest or prejudicial to national security they can be excluded from the report. When the Prime Minister wishes to exclude a section from the report a statement must be provided to Parliament that the section has been excluded.

63. *Subsection (7)* provides for the Secretary of State to pay the independent reviewer expenses incurred in carrying out functions under this section.

64. *Subsection (8)* specifies that the independent reviewer is the person appointed under section 36(1) of the Terrorism Act 2006.

65. Once the independent reviewer has provided his report to the Prime Minister, the additional responsibilities under this section will cease.

COMMENCEMENT DATE AND SUNSET

66. Section 8 provides that the provisions of the Act, other than section 1(6), are commenced on the day of Royal Assent.

67. Section 1(6) is to be commenced by appointed day order. This will allow for the opportunity to identify other organisations that might lose access to retained data subject to this provision, so that other provision can be made in legislation to ensure that vital capabilities are not undermined.

68. The Act will be repealed on 31 December 2016.

HANSARD REFERENCES

69. The following table sets out the dates and Hansard references for each stage of the Act's passage through Parliament.

STAGE	***DATE***	***HANSARD REFERENCE***
House of Commons		
Introduction	14 July 2014	Vol. 584, Cols. 602-603
Second Reading	15 July 2014	Vol. 584, Cols. 704-759
Committee	15 July 2014	Vol. 584, Cols. 760-822
Report and Third Reading	15 July 2014	Vol. 584, Cols. 822-834
House of Lords		
Introduction	16 July 2014	Vol. 755, Col. 599
Second Reading	16 July 2014	Vol. 755, Cols. 599-665
Committee	17 July 2014	Vol. 755, Cols. 707-737
Report	17 July 2014	Vol. 755, Col. 748
Third Reading	17 July 2014	Vol. 755, Col. 748
House of Lords		

STAGE	***DATE***	***HANSARD REFERENCE***
Royal Assent	17 July 2014	Vol. 755, Col. 774
		House of Commons Hansard Vol. 584, Col. 1118