*These notes refer to the Data Retention and Investigatory Powers Bill as introduced in the House of Commons on Monday 14 July 2014 [Bill 73]*

# DATA RETENTION AND INVESTIGATORY POWERS BILL

## EXPLANATORY NOTES

### INTRODUCTION

1. These explanatory notes relate to the Data Retention and Investigatory Powers Bill as introduced in the House of Commons on Monday 14 July 2014. They have been prepared by the Home Office in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.

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

### SUMMARY

3. There is a need to legislate in order to clarify the legislative framework for certain important investigatory powers. Firstly, this Bill 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, legislation is required to clarify 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 Bill 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 components of the Bill are designed to strengthen and clarify, rather than extend, the current legislative framework. Neither component will provide for additional investigatory powers.

4. The first component of the Bill relates to Government requirements for retention of communications data. This is currently provided for in United Kingdom law through the 2009 Regulations. 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 Bill 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 Bill will 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 Bill 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. 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 considers it important to legislate now in order to put beyond any legal doubt the regime for both investigatory techniques.

## BACKGROUND

### Retention of communications data

7. 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.

8. 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.

9. 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.

10. 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.

11. This Bill 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 Bill adds safeguards while providing for the replacement regulations to add further safeguards in line with the judgment.

12. Specifically, the Bill provides 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 Bill 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**

13. 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.

14. Regarding interception, Chapter 1 of Part 1 of RIPA allows for the 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 to ensure 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.

15. This Bill is 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, have questioned whether the legislation 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. It is now important to make that clear on the face of the legislation.

16. The Bill 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.

17. 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 Bill provides the opportunity to make this clear in primary legislation.

18. The Bill 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.

## OVERVIEW

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

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

21. 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.

22. Finally, it provides further clarification of the detail of the definition of a telecommunications service.

## TERRITORIAL EXTENT AND APPLICATION

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

## FAST-TRACK LEGISLATION

24. The Government intends to ask Parliament to expedite the parliamentary progress of this Bill. In their report on *Fast-track Legislation: Constitutional Implications and Safeguards*[1], the House of Lords Select Committee on the Constitution recommended that the Government should provide more information as to why a piece of legislation should be fast-tracked.[2]

### *Why is fast-tracking necessary?*

25. On 8 April 2014, the ECJ declared the Data Retention Directive to be invalid. The United Kingdom's data retention regime is governed by the 2009 Regulations, made under section 2(2) of the European Communities Act 1972, which implemented the Directive. As the EU obligation which the 2009 Regulations implemented has fallen away, it is necessary to urgently make provisions for data retention in United Kingdom law given its importance in protecting the public.

26. Certain provisions of RIPA need to be clarified. This is because companies providing services to individuals within the United Kingdom, but which are not themselves based in the United Kingdom, have questioned whether RIPA applies to them.

27. The Government considers it important to pass legislation quickly to make it unequivocal that the United Kingdom will continue to have a data retention regime and RIPA continues to have extra-territorial jurisdiction. This includes clarifying the definition of a "telecommunications service" to ensure internet-based services, such as webmail, are included.

[1] House of Lords' Constitution Committee, 15th report of session 2008/09, HL paper 116-I
[2] House of Lords' Constitution Committee, 15th report of session 2008/09, HL paper 116-I, para. 186

***What is the justification for fast-tracking each element of the Bill?***

**Fast-tracking data retention elements of the Bill**

28. While the 2009 Regulations still remain in force, the ECJ judgment has resulted in the need for legislation, to put the legal basis for data retention beyond doubt. This legislation also provides an opportunity to implement additional safeguards, where appropriate, in line with the judgment.

29. Retained communications data is of vital importance to law enforcement. It would have a major impact on their work if telecommunications service providers no longer retained data beyond the period they retain it for business purposes. Therefore it is crucial to ensure the regulations governing data retention are on the strongest possible legal footing.

**Fast-tracking amendments to the Regulation of Investigatory Powers Act 2000**

30. The need to clarify the intent of RIPA reflects the increasingly globalised nature of telecommunications. This makes it vital that overseas companies comply with lawful requests made under RIPA. Since RIPA was enacted, there is a greater expectation that where Parliament intends a statute to apply extra-territorially, it will contain explicit provision to that effect. This has resulted in telecommunications companies, which this Bill clarifies includes those that provide internet-based services, such as webmail, questioning whether RIPA can apply to them in the absence of explicit statutory confirmation that it applies extra-territorially. If this clarification is not dealt with quickly, there is an increasing likelihood that telecommunications companies could refuse requests which are critical for national security and the fight against serious crime. It is considered important to clarify urgently the definition of a "telecommunications service" to ensure it captures the range of services that are used by terrorists and criminals in their attack planning and criminal activities.

***What efforts have been made to ensure the amount of time made available for parliamentary scrutiny has been maximised****?*

31. Given the need to ensure that law enforcement agencies are able to retain their capabilities, extending the timetable for parliamentary scrutiny is not possible in this instance. Legislation is being brought forward at the earliest opportunity, having given proper consideration to the implications of the judgment. In order to provide Parliament with the opportunity to scrutinise the detail of these proposals, this has been delegated to secondary legislation, which will be published alongside the Bill and laid before Parliament following Royal Assent.

32. Data retention has been considered in Parliament in relation to the Anti-terrorism, Crime and Security Act 2001, the Retention of Communications Data (Code of Practice) Order 2003, and in relation to the 2007 and 2009 Data Retention Regulations. An expansion of communications data powers was considered by the Joint Committee that scrutinised the Draft Communications Data Bill in 2012. This Bill does not enhance data retention powers, although it is envisaged that when communications data policy is considered in the next Parliament, legislation conferring further powers may be proposed.

33. The measures relating to RIPA are only intended to clarify the intent of the current legislation and therefore were subject to parliamentary scrutiny when RIPA was enacted in 2000.

***To what extent have interested parties and outside groups been given an opportunity to influence the policy proposal?***

34. Due to the pressing nature of this legislation a limited process of consultation has been completed with those affected by the provisions, including the communications industry, and law enforcement and intelligence agencies.

35. Following the judgment of the ECJ, many stakeholders have expressed a desire for clarity as to the legal status of data retention. This Bill provides that clarity.

36. With respect to the clarification of the extra-territorial jurisdiction of RIPA, the suggestion from service providers based overseas that, in the absence of explicit extra-territorial effect, it is not clear that RIPA applies to them has contributed to the need for legislation.

***Does the Bill include a sunset clause (as well as any appropriate renewal procedure)? If not, why does the Government judge that their inclusion is not appropriate?***

37. Yes. This Bill is subject to a sunset clause. The legislation will be repealed on 31 December 2016.

***Are mechanisms for effective post-legislative scrutiny and review in place? If not, why does the Government judge that their inclusion is not appropriate****?*

38. Given the ongoing need to address declining law enforcement capabilities in relation to the changing nature of communications and this sunset clause, a wider review of these investigatory powers is expected in the next Parliament.

***Has an assessment been made as to whether existing legislation is sufficient to deal with any or all the issues in question?***

39. Yes. Regarding data retention, as the 2009 Regulations were based on the now invalid Data Retention Directive it is important to pass enabling legislation to allow for their replacement in United Kingdom law.

40. The Anti-terrorism, Crime and Security Act 2001 provided for data retention through a voluntary code. As the code is voluntary, and the retention periods more limited, the amount of data that would be retained would not be a substitute for a mandatory retention regime.

41. Regarding the amendments to RIPA, in view of the suggestion by overseas telecommunications service providers that the extra-territorial effect of RIPA is unclear, it is considered necessary to amend the legislation to put the issue beyond doubt. This includes clarifying the definition of a "telecommunications service" to ensure the full range of telecommunications services available to customers in the United Kingdom are included in the definition.

***Has the relevant parliamentary committee been given the opportunity to scrutinise the legislation?***

42. Due to time constraints the Home Affairs Select Committee has not had an opportunity to scrutinise the legislation, although details of the provisions have been shared. Delegating the detail of the data retention provisions to secondary legislation will allow Parliament the opportunity to scrutinise that detail. A draft of the regulations will be made available to Parliament during the Bill's passage.

## COMMENTARY

### *Retention of relevant communications data*

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

43. *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 clause 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). Clause 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.

44. The purpose of accessing communications data in the interests of economic well-being is amended in clause 3 of this Bill.

45. 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.

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

47. *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)). Therefore, data that is three months old at the time of the notice would only be allowed to be retained for a further nine months.

48. *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.

49. *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.

50. *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.

51. *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).

52. *Subsection (7)* permits the Secretary of State to apply the safeguards in the regulations to data that is retained on a voluntary basis under the Anti-terrorism, Crime and Security Act 2001.

**Clause 2: Section 1: supplementary**

53. *Subsection (1)* provides relevant definitions. The Bill 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).

54. *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.

55. *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.

56. *Subsection (4)* provides for the regulations under clause 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.

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

***Investigatory powers***

**Clause 3: Grounds for issuing warrants and obtaining data**

58. *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, this is included on the face of the Bill.

59. *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. This is included on the face of the Bill.

**Clause 4: Extra-territoriality in Part 1 of RIPA**

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

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

62. *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.

63. *Subsection (3)* amends section 11(4) of RIPA. That section 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 that section to make clear the duty applies whether or not the person is in the United Kingdom.

64. *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.

65. *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.

66. *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.

67. *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.

68. *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.

69. *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.

70. *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.

**Clause 5: Meaning of "telecommunications service"**

71. This clause 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.

## FINANCIAL EFFECTS

72. It is considered that the changes within the Bill will have an effect on public expenditure. However, it is considered that these changes will more than break even. Regarding interception, given that this legislation is to put the current position beyond doubt, there are no extra costs. Costs relating to communications data amount to £8.4 million (Present Value over 5 years). More details are provided in published impact assessments.

### Data retention

73. Continuing to require data retention does have costs in comparison with no longer requiring data retention. However, the benefits are expected to significantly outweigh these costs. Break-even analysis has been used to show that the data retention legislation would only have to lead to a small reduction in criminal profits recovered or crimes committed for the policy to break-even.

### Interception

74. Under section 14 of RIPA, the Government already provides a "fair contribution" towards the costs of warranted interception to telecommunications service providers subject to RIPA obligations. As the current regime is simply being affirmed through new legislation, this process will continue as before. Base costs of interception will therefore remain the same.

## PUBLIC SECTOR MANPOWER

75. The provisions contained within the Bill have no substantial effect on public service manpower.

## SUMMARY OF THE IMPACT ASSESSMENT

76. Separate impact assessments on the provisions relating to communications data and interception have been carried out and are published separately. They are both available on the Government website.

### Data retention

77. The measures are intended to clarify the current legislative regime and therefore it is not anticipated they will have a substantial impact.

78. The infrastructure to support the provisions in this Bill already exists.

79. The Government will continue to reimburse the costs for storage of data required to be retained under the legislation.

80. As under the 2009 Regulations and RIPA, this legislation is intended to ensure that no telecommunications service provider is either advantaged or disadvantaged by the continued requirements.

81. There is still the potential for small and micro firms to have obligations placed upon them. However, the requirement for prior consultation will allow the implications and mitigations for any small or micro firms to be discussed, and, in relation to data retention, the cost recovery mechanisms will cover any additional costs.

82. As the policy intention is to maintain the status quo, there will also be no additional impact on small or micro firms.

**Interception**

83. The measures are intended to clarify the current legislative regime and therefore it is anticipated there will be no additional impact.

84. The infrastructure to support the provision of warranted intercept is already in place. In addition, as per section 14 of RIPA, the Government would continue to provide a "fair contribution" towards the costs of warranted interception to telecommunications service providers subject to RIPA obligations.

85. As is the case with the current RIPA regime, under new legislation there is the potential for small and micro firms to have intercept obligations placed on them. However, existing safeguards, the "fair contribution" provision enacted under section 14 of RIPA, and prior consultation before obligations are imposed will mean that there is no additional impact on small and micro firms.

**Privacy Impact Statements**

86. In relation to data retention, in addressing the ECJ's concerns, where possible, the new legislation will go even further in safeguarding privacy. It is assessed that implementation of the proposed legislation is capable of being fully compliant with the Data Protection Principles and the Data Protection Act 1998.

87. With regards to interception, this legislation is clarifying the status quo. There will be no new privacy risks associated with the interception provisions in this legislation.

88. The UK already has one of the most stringent oversight and authorisation systems for investigatory powers in the world.

## COMPATIBILITY WITH THE EUROPEAN CONVENTION OF HUMAN RIGHTS

89. Section 19 of the Human Rights Act 1998 requires a minister in charge of a Bill in either House of Parliament to make a statement about the compatibility of the Bill with the Convention rights (as defined by section 1 of that Act).

90. The Home Secretary has made the following statement:

> "In my view the provisions of the Data Retention and Investigatory Powers Bill are compatible with the Convention rights."

91. The Government has published a separate memorandum on ECHR issues with an assessment of compatibility of the Bill's provisions with the Convention rights: this memorandum is available on the Government website. The memorandum is summarised below.

### Data Retention

92. A requirement to retain communications data engages the right to private life and confidentiality of communications in Article 8 of the European Convention on Human Rights. Any interference with that right will be in accordance with the law, because there will be clear provision in legislation governing the requirement on operators to retain communications data (in the new legislation), and the circumstances in which the communications data may be obtained by relevant public authorities (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. 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.

### Interception

93. The Regulation of Investigatory Powers Act 2000 was designed to be compliant with the European Convention on Human Rights. The proposed amendments do not seek to extend the scope of the existing powers or provisions of the 2000 Act, but simply clarify that it has extra-territorial jurisdiction, clarify the services which are captured by the definition of a "telecommunications service", and add the national security consideration to the economic well-being purpose in primary legislation. The provisions of the Bill in respect of interception are compatible with Article 8 of the Convention.

## COMMENCEMENT DATE AND SUNSET

94. Clause 6 provides that the provisions of the Bill, other than clause 1(6), are to be commenced on the day of Royal Assent.

95. Clause 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.

96. The Bill will be repealed on 31 December 2016.

# DATA RETENTION AND INVESTIGATORY POWERS BILL

# EXPLANATORY NOTES

*These notes refer to the Data Retention and Investigatory Powers Bill as introduced in the House of Commons on 14 July 2014 [Bill 73].*

---

*Ordered, by* The House of Commons,
*to be Printed*, 14 *July* 2014.

---



PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS
LONDON — THE STATIONERY OFFICE LIMITED
Printed in the United Kingdom by The Stationery Office Limited
£x.xx

Bill 73—EN 55/4