EXPLANATORY MEMORANDUM TO

THE RETENTION OF COMMUNICATIONS DATA (CODE OF PRACTICE) ORDER 2015

2015 No. [DRAFT]

AND

THE REGULATION OF INVESTIGATORY POWERS (ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA: CODE OF PRACTICE) ORDER 2015

2015 No. [DRAFT]

1. This explanatory memorandum has been prepared by the Home Office and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 This explanatory memorandum concerns orders bringing into force two codes of practice: a new Retention of Communications Data Code of Practice ('the retention code') and a revised Acquisition and Disclosure of Communications Data Code of Practice ('the acquisition code'). Both of these codes are being brought into force to enhance safeguards and ensure clear guidance on best practice with respect to acquisition and retention of communications data.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

4. Legislative Context

4.1 On 8 April 2014 the European Court of Justice ('ECJ') declared the Data Retention Directive (2006/24/EC) ("the Directive") invalid. In response to this judgment, in July 2014, Parliament passed the Data Retention and Investigatory Powers Act ('DRIPA'). Part 1 of DRIPA provides for the Secretary of State, by notice, to require the retention of communications data by communications service providers. The Data Retention Regulations 2014 ("the Regulations"), made under section 1 of DRIPA, provide further detail about the retention of such data. The Regulations provide the provisions of section 71 of the Regulation of Investigatory Powers Act 2000 ('RIPA'), relating to the issuing by the Secretary of State of certain codes of practice, apply with modifications to include a code of practice on data retention.

4.2 Chapter 2 of Part 1 of RIPA provides a statutory framework governing the acquisition of communications data by "relevant public authorities", and its disclosure by postal or telecommunications operators, consistent with the Human Rights Act 1998. There is currently a code of practice on acquisition, made pursuant to section 71 of RIPA. During the passage of DRIPA, the Government also committed to revising the acquisition code of practice.[1] These codes set out how the legislation is implemented in practice.

4.3 The Counter Terrorism and Security Act 2015 ('CTSA') amended DRIPA to allow some additional types of data – namely those which identify the IP address which belongs to the sender or recipient of a communication – to be retained.

5. Territorial Extent and Application

5.1 These codes apply to all of the United Kingdom. Where there are limits on application to Scotland or Northern Ireland (or alternative domestic provision), this is clearly stated in the codes.

6. European Convention on Human Rights

6.1 James Brokenshire MP, Minister for Immigration and Security, has made the following statement regarding Human Rights:

"In my view the provisions of the Regulation of Investigatory Powers (Acquisition and Disclosure of Communications Data: Code of Practice) Order 2015 and the Retention of Communications Data (Code of Practice) Order 2015 are compatible with the Convention rights."

7. Policy background

7.1 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. It is a crucial tool in investigations into numerous offences.

7.2 Communications data policy can broadly be split into two areas: retention and acquisition. If data is not retained, it cannot be accessed. Communications data is collected by communications service providers ('CSPs') for their business purposes, such data can be accessed by law enforcement, the intelligence agencies and other relevant public authorities. However, considering the importance of communications data to those

[1] House of Lords Hansard, 29 July 2014 (Col 1530)

authorities, the Government can require, when necessary and proportionate, relevant data to be retained by CSPs that they do not require for business purposes. Communications data retained for business purposes, or under data retention legislation, can be accessed under RIPA, when necessary and proportionate.

- **The new retention code - What is being done and why?**

7.3 DRIPA and the Regulations made under it replaced the UK's previous data retention regime, while adding a number of safeguards. One of these important changes provided for a statutory code of practice on communications data retention in order to provide clear guidance on best practice.

7.4 The new retention code sets out how the Government implements the requirements in DRIPA and the Data Retention Regulations. It covers the issue, review, variation and revocation of data retention notices; the CSPs' ability to recover their costs; data security; oversight by the Information Commissioner; and safeguards on the disclosure and use of retained data by CSPs. It also outlines the scope and definitions of relevant communications data, including data that may be retained following provisions in CTSA.

- **The revised acquisition code - What is being done and why?**

7.5 The main changes to the acquisition code concern the provision of additional safeguards. The code enhances the operational independence of authorising officers in relevant public authorities. Further changes include reflecting the additional requirements on local authorities to request communications data through a magistrate and the National Anti-Fraud Network; new record keeping requirements for public authorities; and aligning the code with best practice regarding providing communications data to the emergency services following an emergency call.

7.6 The Interception of Communications Commissioner has recommended that judicial approval should be applied where the police request communications data in order to identify a journalist's source. The acquisition code therefore requires the police to use a Production Order under the Police and Criminal Evidence Act 1984 ('PACE'), which requires judicial approval, rather than RIPA, to request communications data in such circumstances. It also specifies that additional consideration to the level of intrusion must be given, in terms of both privacy and, where applicable, freedom of expression, when considering whether to acquire communications data involving professionals who handle privileged or otherwise confidential material.

8. Consultation outcome

8.1 A public consultation which took place between 9 December 2014 and 20 January 2015 invited views on the codes of practice. The Government received around 300 submissions from organisations and individuals suggesting amendments to the codes. The vast majority of these related wholly or primarily to access to the communications data of journalists and others in professions which may be subject to professional privilege. The

Department considered all of the responses to the consultation and many of the suggestions have been adopted in the final drafts, including, in the acquisition code, enhanced safeguards in line with the concerns raised by journalists. The codes also take account of the recent report and recommendations of the Interception of Communications Commissioner on access to the communications data of journalists.

9. Guidance

9.1 These codes of practice provide for the issuing of further advice, where appropriate.

10. Impact

10.1 The impact of these codes on business, charities or voluntary bodies is cost neutral.

10.2 The impact on the public sector is minimal.

10.3 An Impact Assessment has not been prepared for this instrument. Full impact assessments were carried out for the Data Retention and Investigatory Powers Act 2014 and the Counter-Terrorism and Security Act 2015.

11. Regulating small business

11.1 The legislation applies to small business.

11.2 Impact on small business is mitigated in that firms complying with either requests for communications data, or being required to retain communications data, are reimbursed by the Government. Charter 5 in the retention code and Chapter 4 in the acquisition code outline these arrangements.

12. Monitoring & review

12.1 Section 7 of DRIPA requires the Independent Reviewer of Terrorism Legislation carry out a review of investigatory powers, including communications data. This review, if reasonably practicable, will be completed by 1 May 2015. DRIPA also contains a sunset clause. It will be repealed on 31 December 2016. The data retention code of practice will accordingly cease to have effect when DRIPA is repealed.

13. Contact

Lucy Montgomery-Pott, Home Office, Tel: 020 7035 6634, email: lucy.montgomery-pott@homeoffice.x.gsi.gov.uk, can answer any queries regarding the instrument.