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

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.