EXPLANATORY MEMORANDUM TO

THE DATA RETENTION AND ACQUISITION REGULATIONS 2018

2018 No. [XXXX]

1. Introduction

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

2. Purpose of the instrument

2.1 The Regulations amend the legislative scheme providing for the retention of and access to communications data – information about communications, but not its content. Legislative changes are required to ensure the United Kingdom's communications data retention regime complies with European Union law.

2.2 The Regulations also bring into force the Communications Data Code of Practice under the Investigatory Powers Act 2016 (IPA).

3. Matters of special interest to Parliament

Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None.

Other matters of interest to the House of Commons

3.2 Disregarding minor or consequential changes, the territorial application of this instrument includes Scotland and Northern Ireland.

4. Legislative Context

4.1 In response to two cases[1] referred to the Court of Justice of the European Union (CJEU), including a reference from the Court of Appeal, the CJEU specified a number of requirements that need to be in place for a communications data retention regime to be compliant with EU law (see section 7, below).

4.2 Amendments are required to Parts 3 and 4 of the IPA and to Chapter 2 of Part 1 of Regulations of Investigatory Powers Act 2000 in response to the CJEU judgment.

4.3 These Regulations also bring into force a code of practice in accordance with the requirement in Schedule 7 of the IPA. Paragraph 1 of Schedule 7 requires the Secretary of State to issue codes of practice about the exercise of functions conferred by virtue of the IPA.

4.4 Part 4 of the IPA provides for the retention of communications data by telecommunications and postal operators so it is available for subsequent access by public authorities when authorised under the provisions in the Regulation of Investigatory Powers Act 2000 (RIPA) (and in future under the IPA).

[1] C-203/15 Tele2 Sverige AB v Post – och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others

4.5 Chapter 2 of Part 1 of RIPA (Acquisition and Disclosure of Communications Data) provides a statutory framework governing the acquisition of communications data by public authorities, and its disclosure by telecommunications or postal operators. Section 22(2) provides a list of statutory purposes for which communications data can be acquired.

4.6 The provisions for the acquisition of communications data in RIPA will be replaced by those in Part 3 of the IPA in due course. Part 3 of the IPA will then govern the acquisition of communications data.

4.7 Paragraph 6 of Schedule 7 to the IPA sets out the effect of the codes of practice. A person must have regard to the codes when exercising any functions to which the codes relate. The codes are admissible as evidence and a court or tribunal may take into account a failure to have regard to them.

5. Extent and Territorial Application

5.1 The extent of this instrument is all of the United Kingdom.

5.2 The territorial application of this instrument is the whole of the United Kingdom.

6. European Convention on Human Rights

6.1 The Rt. Hon. Ben Wallace MP has made the following statement regarding Human Rights:

"In my view, the provisions of the Data Retention and Acquisition Regulations 2018 are compatible with Convention Rights."

7. Policy background

What is being done and why

7.1 This section explains (i) what communications data is, and why it is retained, (ii) what powers have been engaged in retention and access, (iii) how that is affected by the judgment from the CJEU, and (iv) why the Government needs to make amendments to the IPA.

7.2 Communications data is generated by telecommunications and postal operators in the course of their business practices. It can then 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 telecommunication was made. It does not include the content of any communication: for example the text of an email, or what was said on a phone call. Access to communications data is essential for law enforcement and national security investigations.

7.3 Data protection law requires operators to delete data that they no longer require for business purposes. It is therefore necessary to have a power to require the retention of data. Section 87(1) of the IPA provides such a power. It gives the Secretary of State the ability, by notice, to require the retention of communications data for purposes such as the prevention and detection of crime. Essentially, if data is not retained, it cannot be accessed subsequently. Sometimes communications data is the only way to identify offenders. Given its importance to investigations, it is crucial to ensure that it is retained where it is necessary and proportionate to do so, for up to a year, and that it can then be accessed by the relevant public authority under strict controls.

7.4 Under RIPA, specified types of communications data can be accessed by relevant public authorities where necessary and proportionate for one of the statutory purposes. These purposes include national security, prevention and detection of crime, public safety, and preventing death and injury. These are consistent with the purposes for which data can be retained. Requests are currently authorised by an operationally independent designated person, a rank stipulated by Parliament, within the requesting authority. These provisions are broadly replicated in Part 3 of the IPA, although these provisions have not yet commenced and are now subject to amendment through these Regulations.

7.5 Following the CJEU judgment in December 2016 (*Tele2/Watson*), the Government accepted that amendments were needed to the Investigatory Powers Act to make it consistent with EU law. In particular (i) to provide for independent administrative or judicial authorisation for most communications data applications, and (ii) restricting the crime purpose for acquiring retained communications data to serious crime.

7.6 These Regulations provide for a number of amendments to the IPA including provisions:

- for independent authorisation of most communications data requests;
- for internal authorisation of requests in urgent cases, and in cases of national security and where the request is being made by the three intelligence agencies;
- restricting the crime purpose for which events data (such as call histories and location information) can be retained and acquired, to a new threshold of serious crime;
- further restricting the purposes for which data can be acquired and retained by removing three statutory purposes; and
- adding additional considerations that must be taken into account by the Secretary of State before a retention notice is given.

7.7 The above provisions are explained in further detail at paragraphs 7.9 – 7.16, below.

7.8 The Divisional Court has required that the legislative regime should be amended by 1 November 2018 although the Court has accepted that, due to the complexity of implementation, the requirement for independent authorisation of communications data requests will take until April 2019.

7.9 The Government intends to commence the new serious crime threshold, which is not subject to the same implementation complexities, in November 2018. Accordingly corresponding amendments are required to RIPA which will remain the regime governing access to communications data until Part 3 of the IPA, and the associated requirements for independent authorisation, come into force in April 2019. The corresponding amendments will:

- restrict the crime purpose for which traffic and service use data (which is the equivalent of events data under the IPA) can be acquired under RIPA to a new threshold of serious crime; and
- further restrict the purposes for which data can be acquired under RIPA by removing three statutory purposes (see paragraph 7.14, below).

Independent authorisation

7.10 The Regulations create a new power for the Investigatory Powers Commissioner (IPC) to authorise most communications data requests. The IPC will delegate these functions to a newly appointed body of staff, to be known as the Office for Communications Data Authorisations (OCDA). OCDA will report directly to the IPC, and will be responsible for considering the vast majority of requests to access communications data made by public authorities. The Regulations also provide for the replacement of Magistrates approval for local authority requests under the current regime with authorisation by OCDA to ensure for a single consistent regime of independent authorisation.

Internal authorisation in urgent cases

7.11 The CJEU judgment recognises that it is acceptable for public authorities to authorise requests internally in cases of validly established urgency. As such, the Government has proposed provisions in the regulations which allow for internal authorisation by a designated senior officer in a public authority where there is an urgent need to obtain communications data. Internal authorisation of requests will be available to all public authorities except local authorities, who will be prohibited from authorising communications data requests internally for any purpose. This reflects the additional level of scrutiny Parliament deemed appropriate for those bodies in the IPA.

Internal authorisation in other cases

7.12 The Government takes the view that the CJEU judgment does not cover requests for communications data made for national security purposes or for requests made by one of the three intelligence agencies As such, the current internal authorisation regime for these cases will be maintained under the new regime. Where an intelligence agency makes a request or another public authority makes a request for the purpose of national security or the economic well-being of the UK so far as it relates to national security, these cases can be authorised by a designated senior officer within the public authority. As now, the designated senior officer will need to be independent of the investigation except in the limited circumstances currently defined in the Act.

Serious crime

7.13 The CJEU judgment required that where traffic and location data (called events data in the IPA) are retained or acquired for the purpose of the prevention and detection of crime, this should be restricted to serious crime. The Regulations therefore provide a definition of serious crime for the purposes of the retention or acquisition of events[2] data under the IPA. The threshold will be met for investigations into all offences for which an adult is capable of being sentenced to twelve months or more in prison; any offence involving violence; any offence which involves a large number of people acting in pursuit of a common purpose; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or any offence involving a significant financial gain. The regulations apply the same threshold to the acquisition of traffic and service use data under RIPA. Traffic and service use data is the equivalent of events data under the modernised definitions in the IPA.

Restricting the statutory purposes

[2] Any data which identifies or describes an event (whether or not by reference to its location) on, in, or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at a specific time.

7.14 The Regulations will also remove three of the statutory purposes for which communications data can be retained and acquired; namely:

- Public health;
- Collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; and
- Exercising functions relating to the regulation of financial services and markets, or financial stability.

7.15 The Government proposes removing the above three purposes because they could allow for communications data to be retained or acquired in relation to criminal activity that would not meet the serious crime threshold required by the CJEU.

Additional considerations for the Secretary of State when issuing a retention notice

7.16 The Government proposes to amend the list of factors that the Secretary of State must take into account when giving a data retention notice to a telecommunications operator or postal operator to include additional factors. This will ensure the data retention regime is clear and transparent, and will place beyond any doubt that our data retention regime is consistent with the requirement in the CJEU judgment for a regime not to be general and indiscriminate. The additional factors are:

- requiring that a notice must specify the services to which it relates, and that the Secretary of State must specifically consider which of the operator's services the notice relate to;
- requiring consideration of whether it would be appropriate to restrict a notice by geography, or exclude groups of customers; and
- more closely linking the benefits of the notice to the statutory purpose by ensuring the Secretary of State takes into account the statutory purpose(s) for which the notice is being given when considering the potential benefits of the notice. For example, the Secretary of State will need to consider how the retention of data would be beneficial in the prevention and detection of serious crime, rather than how the retention of the data would be beneficial more generally.

Code of practice

7.17 Schedule 7 to the Act requires codes of practice about the exercise of the functions conferred by the Act to be issued. These regulations will bring into force the Communications Data Code of Practice which relates to the powers and duties conferred or imposed under Parts 3 and 4 of the IPA.

7.18 The Code, which takes account of the changes made by these Regulations to the statutory scheme, provides guidance on:

- procedures to be followed for the acquisition of communications data;
- rules for the granting of authorisations to acquire data and the giving of notices to require disclosure of data;
- procedures to be followed for the retention of communications data;
- security principles which must be adhered to by those retaining data;
- keeping of records, including records of errors; and
- the oversight arrangements in place for acquisition and retention of communications data.

7.19 In response to the CJEU judgment, the code also provides guidance on:

- when data can be transferred in and out of the EU; and
- the circumstances in which notification of individuals, that their communications data has been acquired, can take place under the new regime

7.20 The code is aimed at members of public authorities who are involved in the acquisition of communications data whether as an applicant, a single point of contact, a designated senior officer or a senior responsible officer; and staff within telecommunications operators and postal operators who are involved in the lawful disclosure of communications data or who currently, or may in the future, retain data under the Act.

8. Consultation outcome

8.1 On 30 November 2017, the Government held a public consultation on proposed changes to the regime and on the code of practice. The consultation closed on 18 January 2018. 794 responses were received, of which 716 were a direct result of a campaign run by the digital campaigning organisation Open Rights Group, which encouraged its supporters to submit their views based on areas of concern expressed by Open Rights Group. The remaining 78 submissions were made by academics, members of the public, legal representatives, public authorities, telecommunications and postal operators, media groups, oversight bodies and civil society groups

The responses that we received provided useful and constructive feedback. Some recurring themes that emerged from the consultation related to the threshold for serious crime, the application of the CJEU judgment to the less intrusive 'entity' data, and the requirement for notification. The Government has increased the serious crime threshold from six to 12 months as a result, and made further minor amendments to aid clarity. A summary of these concerns and the Government response can be found at https://www.gov.uk/government/consultations/investigatory-powers-act-2016.

9. Guidance

9.1 The Code of Practice being brought into force by these Regulations provides guidance on the powers in Parts 3 and 4 of the IPA, as amended by these regulations, as well as guidance on the effect of the codes. The Home Office has also published a statutory code of practice providing guidance on the operation of Chapter 2 of Part 1 of RIPA, and has provided internal guidance to public authorities on the effect of the amendments in these Regulations.

10. Impact

10.1 There is no impact on business, charities or voluntary bodies because these Regulations relate to additional safeguards in accessing communications data by law enforcement agencies, and in the issue of retention notices by the Secretary of State.

10.2 The impact on the public sector is set out in full in the policy consideration section above. In short, most requests for communications data by public authorities, such as law enforcement bodies, will be authorised by the new Office for Communications Data Authorisations rather than under the current internal authorisation procedure.

10.3 An Impact Assessment is submitted with this memorandum and will be published alongside the Explanatory Memorandum on the legislation.gov.uk website. A full

impact assessment was also carried out for the IPA and is available on the legislation.gov.uk website.

11. Regulating small business

11.1 The legislation applies to activities that are undertaken by small businesses. However they relate to additional safeguards for accessing retained communications data, and on the issue of retention notices to telecommunications operators and postal operators.

11.2 The Regulations in and of themselves do not impose requirements on small businesses, rather they set out obligations that could be imposed on a telecommunication or postal operator through a data retention notice. To minimise the impact of the requirements on small businesses (employing up to 50 people), the approach taken is that the IPA provides that all telecommunications operators that are required to retain or disclose communications data are entitled to recovery of reasonable costs of complying with the those requirements. Also, there are safeguards regulating the use of data retention notices in the Act, including that the notice must be necessary, proportionate and approved by a judicial commissioner.

12. Monitoring & review

12.1 Section 90(13) of the IPA requires the Secretary of State to keep individual retention notices under review.

12.2 Section 260 of the IPA requires the Secretary of State to report on the operation of the Act, after a period of 5 years and 6 months from Royal Assent. The report must be published and laid before Parliament. In preparing the report, the Secretary of State must take into account any report on the operation of the Act produced by a select committee of either House.

12.3 The Investigatory Powers Act provides for an Investigatory Powers Commissioner whose remit includes providing comprehensive oversight of the use of the powers contained within the Act.

13. Contact

13.1 James Dix at the Home Office; commsdata@homeoffice.x.gsi.gov.uk can answer any queries regarding the instrument.