EXPLANATORY MEMORANDUM

THE REGULATION OF INVESTIGATORY POWERS (COMMUNICATIONS DATA) ORDER 2003

European Convention on Human Rights

In the view of the Parliamentary Under Secretary of State for the Home Department, Caroline Flint, the provisions of the above Order are compatible with the Convention Rights.

Powers exercised

The above instrument is made in exercise of the powers conferred by, paragraph (g) of the definition of "relevant public authority" in section 25(1), and section 25(2) and (3) of the Regulation of Investigatory Powers Act 2000 (RIPA). It cannot have effect until it is approved by resolution of each House of Parliament and will not come into effect until one month after it is made.

Legislative background

Chapter II of Part I of RIPA (acquisition and disclosure of communications data) gives public authorities the power to acquire communications data. It introduces a statutory framework to regulate access to communications data by public authorities consistent with the Human Rights Act 1998. It explains the duties and responsibilities placed upon each party involved in the process and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (ECHR).

Section 25(1) of RIPA defines "relevant public authorities" for the purposes of Chapter II of Part I of that Act. Paragraph (g) of the definition of "relevant public authority" in section 25(1) permits the Secretary of State to add further public authorities to this list by means of an Order subject to the affirmative resolution procedure in Parliament.

Section 25(5) of RIPA requires that the Secretary of State shall not make an Order adding public authorities unless a draft has been laid before Parliament and approved by a resolution of each House.

Section 25(2) of RIPA designates authorising officers for relevant public authorities and section 25(3) places restrictions on them. Schedules 1 and 2 in the attached draft Order lists each existing and additional public authority, the authorising officer(s) who can grant authorisations or give notices for communications data, the types of communications data that can be acquired and the purposes under section 22(2) of RIPA for which communications data may be acquired by that authority. Chapter II is not yet in force and it is intended to commence it on the date this Order will take effect if approved.

Article 3 to this Order adds the following public authorities to Chapter II of Part I of RIPA to acquire communications data.

Additional public authorities who can acquire all types of communications data:

- Scottish Drug Enforcement Agency (successor to the Scottish Crime Squad)
- United Kingdom Atomic Energy Authority Constabulary
- Fire Authorities
- Emergency Ambulance Services
- Maritime and Coastguard Agency
- Financial Services Authority
- Office of the Police Ombudsman for Northern Ireland
- Department of Trade and Industry: Radiocommunications Agency

Additional public authorities who can only acquire communications data falling within section 21(4)(b) and (c) of RIPA e.g. itemised billing or subscriber data respectively. (This excludes these authorities from acquiring communications "traffic" data as defined in section 21(4)(a) of RIPA e.g. mobile phone location data.):

- Charity Commission
- Common Services Agency for the Scottish Health Service: NHSScotland Counter Fraud Services
- Department of Enterprise, Trade and Investment for Northern Ireland: Trading Standards Service
- Department for Environment, Food and Rural Affairs: Investigation Branch; Centre for Environment, Fisheries and Aquaculture Science; Counter Fraud and Compliance Unit of the Rural Payments Agency
- Department of Health: Medicines and Healthcare Products Regulatory Agency
- Department of Trade and Industry: Companies Investigation Branch; Legal Services Directorate D

- Environment Agency
- Food Standards Agency
- Gaming Board for Great Britain
- Health and Safety Executive
- Home Office: Immigration Service
- Information Commissioner
- Local authorities (explicitly excluding Parish Councils, Community Councils and the Greater London Authority)
- NHS Counter Fraud and Security Management Service
- Northern Ireland Health and Social Services Central Services Agency: Counter Fraud Unit
- Office of Fair Trading: Cartel Investigations Branch
- Postal Services Commission
- Royal Mail Group plc
- Scottish Environment Protection Agency
- Serious Fraud Office

Column 2 of Schedules 1 and 2 prescribes the designated officers for the relevant public authorities with column 3 prescribing the designated officers for data falling within section 21(4)(c) of the Act, commonly referred to as subscriber data. These senior designated persons of the relevant public authorities can only acquire communications data for the ground(s) listed alongside their entry in column 4.

Furthermore, Article 7(1) and (3) of the Order stipulates that other than for the purposes of in the interests of national security, preventing and detecting crime or preventing disorder, in the interests of the economic well-being of the United Kingdom, or preventing death or injury in an emergency, the only data that can be obtained for any of the other purposes in section 22(2) of RIPA is data falling within section 21(4)(c) e.g. subscriber data.

Policy background

The Home Office consultation paper *Access to communications data – respecting privacy and protecting the public from crime*, published in March 2003, set out proposals for public authorities' access to communications data under RIPA. Responses to the consultation paper show broad support for public authorities having necessary and proportionate access to communications data for the purposes of reducing crime and helping the emergency and rescue services to save lives. Respondents expressing an opinion overwhelmingly favoured the clarity of a single regulatory regime.

The public authorities listed in Schedules 1 and 2 to the Order have responsibility variously for protecting national security; for preventing or detecting crime or preventing disorder; to protect the interests of the economic well-being of the United Kingdom; to protect public health and public safety; assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; and in an emergency to prevent death or injury. The purpose of this Order is to provide those public authorities that carry out these functions with statutory European Convention on Human Rights (ECHR) cover for their activities.

Communications data is information held by communication service providers (eg telecom, Internet and postal companies) relating to the communications made by their customers. This includes itemised call records, routing information and subscriber details. Communications data does not include the content of any communication.

Chapter II of Part I of RIPA provides that within each relevant public authority only persons holding certain offices, ranks or positions may grant authorisations or give notices requiring communications data. For both additional public authorities and those already on the face of the Act these senior offices, ranks and positions are designated by the Secretary of State in this Order. The Order also places restrictions on the types of communications data that can be accessed and the purposes for which data can be accessed.

Schedule 1 of the Order list those public authorities that are currently included in Chapter II of Part I of the Act for the purposes of acquiring communications data, whereas Schedule 2 lists additional public authorities for this purpose. Within Schedule 2, Part I lists those additional public authorities with access to all types of data. Part II lists the authorities in Part I that may only acquire data falling within section 21(4)(b) and (c) of the Act (commonly referred to as itemised call or billing data and subscriber data respectively) for crime and public safety purposes only. Part III lists the majority of additional public authorities who can only access data falling under section 21(4)(b) and (c). Part IV lists the additional public authorities who can only acquire postal communications data.

For the statutory purposes set out in section 22(2) of RIPA other than national security, crime, economic well-being of the United Kingdom, preventing death or injury in an emergency, the only communications data that may be acquired is data falling within section 21(4)(c) of RIPA (subscriber data).

In all cases communications data may only be acquired if they are necessary on one or more of the statutory grounds listed in section 22(2) of RIPA and as

limited by column 4 of Schedules 1 and 2 to the Order. Acquiring data must be proportionate to what is sought to be acheived by so obtaining it.

A statutory code of practice on acquisition of communications will set out the procedures to be followed, including the information to be contained in an application and notices for communications data, by the relevant public authorities.

Oversight of the Chapter II Part I provisions is provided by the Interception of Communications Commissioner by virtue of section 57 of RIPA. The Investigatory Powers Tribunal established by section 65 of RIPA is the appropriate forum for all complaints to be addressed.

Financial effects

Section 24 of the Act allows for payment arrangements to be made in order to compensate holders of communications data for the costs involved in complying with the notices issued under Chapter II of Part I of RIPA. This may include arrangements for payments to be made out of money provided by Parliament.

(Currently, agreements are in place between communications service providers and public authorities that provide for cost recovery where a service provider is called upon to provide communications data. The agreements have been reached independently of the Government and take account of the fact that a requirement to provide communication data places operational and financial burdens on the service provider).

Jurisdiction

This instrument applies to the United Kingdom.