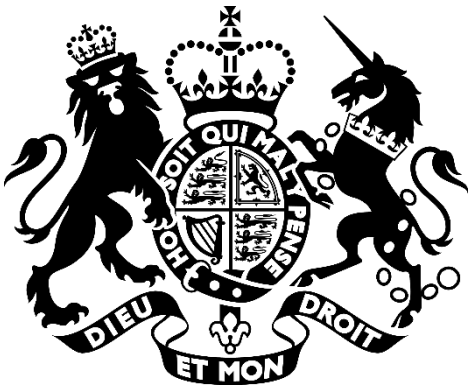
Home Office

Notices Regime

Code of Practice

[Draft for consultation]

[leave this page blank – back of cover]



Notices Regime

Investigatory Powers Act 2016 Code of Practice

Presented to Parliament
by the Home Secretary
by Command of Her Majesty

[Autumn 2024]

CM XXXX

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at publicenquiries@homeoffice.gov.uk.

ISBN XXX-X-XXXX-XXXX-X

XXXXXXXXXXXXX MM/YY

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of
the Controller of Her Majesty’s Stationery Office

Contents

[leave this page blank – back of contents page]

Introduction

1. Introduction

1.1. This Code of Practice relates to the powers and duties conferred or imposed under Part 4 and sections 249 and 252 to 258B of Part 9 of the Investigatory Powers Act 2016 ("the Act").

1.2. The Code of Practice sets out further detail on the circumstances in which a data retention, technical capability, national security, or notification notice can be given; the process that must be followed before a notice can be given; the obligations that may be imposed by the giving of a notice and the ensuing right of review; and oversight of the use of notices.

1.3. The Act provides that all Codes of Practice issued under Schedule 7 to the Act are admissible as evidence in criminal and civil proceedings. If any provision of this Code appears relevant before any court or tribunal considering any such proceedings, or to the Investigatory Powers Tribunal (IPT), or to the Investigatory Powers Commissioner responsible for overseeing the powers and capabilities conferred by the Act, it may be taken into account.

1.4. For the avoidance of doubt, the duty to have regard to the Code when exercising functions to which the Code relates exists regardless of any contrary content of a relevant operator's internal advice or guidance.

2. Scope and Definition

Telecommunications and Postal Definitions

2.1. A telecommunications operator is a person who:

- offers or provides a telecommunications service to persons in the UK;
- who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK; or
- controls or provides a telecommunication system which is not (wholly or partly) in, or controlled from, the UK and is used by another person to offer or provide a telecommunications service to persons in the UK.[1]

2.2. This definition of a telecommunications operator makes clear that a UK nexus is required.

2.3. Section 261(11) of the Act defines 'telecommunications service' to mean any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service). Section 261(13) defines 'telecommunication system' to mean any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. The definitions of 'telecommunications service' and 'telecommunication system' in the Act are intentionally broad so that it remains relevant for new technologies.

2.4. The Act makes clear that any service which consists in, or includes, facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of a telecommunication system is included within the meaning of 'telecommunications service'.[2] Internet based services, such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition.

2.5. A telecommunications operator also includes application and website providers, but only insofar as they provide a telecommunications service. For example, an online marketplace may be a telecommunications operator if it provides a connection to an application/website. It may also be a telecommunications operator if and in so far as it provides a messaging service.

[1] See Section 261(10) of the 2016 Act.

[2] Section 261(12) of the Act.

2.6. Telecommunications operators may also include persons who provide services where customers, guests or members of the public are provided with access to communications services that are ancillary to the provision of another service, for example in commercial premises such as hotels, or public premises such as airport lounges, or on public transport.

2.7. A postal operator is a person providing a postal service to a person in the UK. This definition makes clear that obligations in the Act cannot be imposed on providers who do not provide postal services to persons in the UK.

2.8. Section 262(7) of the Act defines 'postal service' to mean any service which consists in one or more of the collection, sorting, conveyance, distribution, and delivery (whether in the United Kingdom or elsewhere) of postal items and which is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place.

2.9. For the purposes of the Act a postal item includes letters, postcards, and their equivalents as well as packets and parcels.[3] It does not include freight items such as containers. A service which solely carries freight is not considered to be a postal service under the Act. Where a service carries both freight and postal items it is only considered to be a postal service in respect of the transmission of postal items.

Composition of Communications

2.10. For the purposes of the Act, communications may comprise two broad categories of data: systems data and content. Some communications may consist entirely of systems data and will not therefore contain any content. Section 261(6)(b) makes clear that anything which is systems data is, by definition, not content. Systems data includes communications data as defined in section 261(5).

Communications Data

2.11. The term 'communications data' includes the 'who', 'when', 'where', and 'how' of a communication but not the content e.g., what was said or written. However, there is a subset of "content" which can be considered to be communications data – see section 261(6) and paragraph 2.19 for the definition of "content".

2.12. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio, and video that reveals the meaning, other

[3] Section 262(5) of the 2016 Act.

than inferred meaning,[4] of the communication (unless the content falls within the small subset that may be CD, referred to above).

2.13. It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging, and the use of applications. It also includes postal services.

2.14. Communications data is generated, held, or obtained in the provision, delivery, and maintenance of communications services – e.g., postal services or telecommunications services. Further details can be found in the Communications Data Code of Practice.

Relevant Communications Data

2.15. A data retention notice under the Investigatory Powers Act 2016 may only require the retention of relevant communications data. Relevant communications data is defined in section 87 of that Act and is a subset of communications data.

2.16. It is data which may be used to identify or assist in identifying any of the following:

- the sender or recipient of a communication (whether or not a person) – this can include phone numbers, email addresses, user identities and other information which can identify a customer such as names, addresses, account details and other contact information. In the context of internet access this can include source and destination IP addresses, port numbers and the relevant elements of URLs;[5]

- the time or duration of a communication – this can include the time and duration of phone calls, the time of emails, connections on the internet, or internet access sessions;

- the type, method or pattern, or fact, of communication – this can include billing records or other records showing the usage of a communication system;

- the telecommunication system (or any part of it) from, to, or through which, or by means of which, a communication is or may be transmitted – this can

[4] As set out at section 261(6)(a) of the IPA 2016, in relation to the definition of “content”.

[5] See section on web browsing and communications data, paragraphs 2.77-2.85 in the Communications Data Code of Practice

include the identities of cell masts or Wi-Fi access points to which a device has connected; or

- the location of any such system – this can include the physical location of phones or other communication devices or the location of cell masts or Wi-Fi access points to which they connect.

2.17. The data to be retained under a retention notice will be set out in the notice. A notice may provide for the retention of data that is necessary to enable the telecommunications operator or postal operator to correlate the above data and disclose it when required to under Part 3 of the Act. This may include, but is not limited to, customer reference numbers. The data that can be retained under a notice includes the data which would form an internet connection record.

2.18. Section 87(4) of the Act specifies that a retention notice must not require the retention of third-party data, unless that data is, or can only be obtained by processing, an internet connection record (see below). Where the telecommunications operator needs the data for the functioning of a telecommunication system or where the data is retained or used for any other purpose, it is not third-party data. Determining what is third party data and whether it can be separated from other data is complex and will require careful consideration on a case-by-case basis as part of the consultation before a retention notice is given. See paragraphs 4.6 – 4.11 for more information on third-party data.

Content of a Communication

2.19. The content of a communication is defined in section 261(6) of the Act as any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might be reasonably be considered to be the meaning (if any) of that communication.

2.20. When one person sends a message to another, what they say or what they type in a message on a messaging application or the subject line or body of an email for example is the content. However, there are many ways to communicate and the definition covers the whole range of telecommunications. What is consistent is that the content will always be the part of the communication (whether it be the speech of a phone call or the text of an email or a message via a messaging application) that conveys substance or meaning. It is information which conveys that meaning that the Act defines as content.

2.21. When a communication is sent over a telecommunication system it can be carried by multiple operators. Each operator may need a different set of data in order to route the communication to its eventual destination. Where data attached to a communication is identified as communications data it continues to be communications data, even if certain providers have no reason to use this

data (see 'third-party data', at paragraphs 4.6 to 4.11). The definition of content ensures that the elements of a communication which are considered to be content do not change irrespective of which operator is carrying the communication.

2.22. There are two exceptions to the definition of "content" and one type of data that is excluded from the content 'carve out'. The exclusion is found in section 261(5A) and 261(5B), and the exceptions are in section 261(6)(a) and 261(6)(b).

2.23. The exclusion from the content 'carve out', at section 261(5A) and (5B), is in the context of 'relevant subscriber data' and was inserted into the Investigatory Powers Act 2016 by the Investigatory Powers (Amendment) Act 2024. 'Relevant subscriber data' means entity data, other than data comprised in a recording of speech, which constitutes any or all of the content of a communication made for the purpose of initiating or maintaining an entity's access to a telecommunication service and is about an entity to which that telecommunication service is, or is to be, provided. As an example, data submitted within an online form could be considered as providing the 'meaning' of a communication. Section 261(5A) makes clear this type of information is 'relevant subscriber data' where it is for the purpose of initiating or maintaining access to a telecommunications service, and is entity data and communications data (see paragraph 2.26 in the Communications Data Code of Practice). For example, when seeking to identify the driver of a hire car, the driver's name and address details inputted via an online booking form will be communications data and not content. In this example, the hire company is providing the telecommunications 'service' used to book the hire car and the data provided was for the purpose initiating or maintaining access to the telecommunications system through which the car could be booked. If the public authority is unsure whether the communications data has been provided online or in-person to a company representative and entered into an electronic system manually, then they must apply for a Part 3 authorisation or utilise another appropriate lawful authority.

2.24. The first exception to the meaning of "content", at section 261(6)(a), is any meaning that could be inferred from the fact of the communication. When a communication is sent, the simple fact of the communication may convey some meaning, (e.g., it could provide a link between persons or between a person and a service). This exception makes clear that any communications data associated with the communication remains communications data and the fact that some meaning can be inferred from it does not make it content.

2.25. The second exception, at 261(6)(b), makes clear that systems data cannot be content.

Postal Content

2.26. In the postal context, anything included inside a postal item, which is in transmission, will be content. Any message written on the outside of a postal item, which is in transmission, may be content and fall within the scope of the provisions for interception of communications. For example, a message written by the sender for the recipient will be content, but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning its postal routing (e.g., the address of the recipient, the sender, and the post-mark) is postal data and will not be content. In the context of postal communications secondary data is limited to system data.

Interception

2.27. Section 4 of the Act states that a person intercepts a communication in the course of its transmission by means of a telecommunication system if they perform a relevant act in relation to the system and the effect of that act is to make any content of the communication available at a relevant time to a person who is not the sender or intended recipient of the communication. The interception may require the assistance of a telecommunications operator or postal operator, and more information on this is provided at Chapter 7 of the Interception of Communications Code of Practice. Section 4(2) sets out that "relevant act" in this context means:

- modifying, or interfering with, the system or its operation;
- monitoring transmissions made by means of the system;
- monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

2.28. Section 4(4) sets out that a "relevant time" in this context means:

- any time while the communication is being transmitted, and
- any time when the communication is stored in or by the system (whether before or after its transmission).

Equipment

2.29. Equipment is defined in the Act as comprising "any equipment producing "electromagnetic, acoustic or other emissions" and any device capable of being used in connection with such equipment.[6] "Equipment" for these purposes is not

[6] See section 135 in Part 5 and section 198 in Chapter 3 of Part 6 – the definitions are identical.

limited to equipment which is switched on and / or is emitting signals but also includes equipment which is capable of producing such emissions.

2.30. The definition of equipment is technology neutral and encompasses devices that may be thought of as “computers” in the traditional sense as well as the increasing range of “smart” and Internet of Things devices. Examples of the types of equipment captured by the definition include devices that may be regarded as "computers" for the purposes of the Computer Misuse Act 1990[7], such as desktop computers, laptops, tablets, internet-enabled smart devices, and smart systems (including phones, watches, cars, and domestic household devices), other internet-enabled or networked devices and any other devices capable of being used in connection with such equipment. Cables, wires, and storage devices (such as USB storage devices, CDs, or hard disks drives) are also covered as they can also produce "emissions" in the form of an electromagnetic field.

Equipment Data

2.31. An equipment interference warrant may authorise the obtaining of communications, equipment data and other information. Equipment data is defined in the Act and comprises:[8]

- systems data;[9] and
- identifying data which:[10]
  - is comprised in, included as part of, attached to or logically associated with a communication or any other item of information;
  - is capable of being logically separated from the remainder of the communication or item of information; and
  - once separated, does not reveal anything of what might reasonably considered to be the meaning (if any) of the communication or item of information.

2.32. **Systems data** means any data that enables, or facilitates, or identifies and describes anything connected with enabling or facilitating, the functioning of any systems or services. Systems data that is necessary for the provision and operation of a service or system also includes the data necessary for the

[7] The term "computer” is not defined in the CMA; rather the Act relies on the ordinary meaning of the word in the relevant context.

[8] See section 100 in Part 5 and section 177 in Chapter 3 of Part 6 – the definitions are identical.

[9] See section 263(4) for the definition of systems data.

[10] See section 263(2) and (3) for the definition of identifying data.

storage of communications and other information on relevant systems.[11] Systems data includes communications data as defined in section 261.

2.33. Examples of systems data could be:

- messages at rest or in the course of transmission between items of network infrastructure to enable the system to manage the flow of communications;
- router configurations or firewall configurations;
- software operating system (version);
- unique identifiers that facilitate the operation of a service or system such as MAC (medium access controller) addresses, IP (internet protocol) addresses, and SSIDs (Service Set Identifier) but also user identifiers such as email addresses, usernames, screen names, and other, similar account identifiers; and
- the period of time a router has been active on a network.

2.34. **Identifying data** is data which may be used to identify or assist in identifying:

- any person, apparatus, system or service;
- any event; or
- the location of any person, event, or thing.

2.35. In many cases identifying data will also be systems data, however, there will be cases where this information does not enable or otherwise facilitate the functioning of a service or system and therefore is not systems data.

2.36. Identifying data will only be equipment data if it is comprised in, included as part of, attached to or logically associated with a communication or any other item of information and can be logically separated from the remainder of the communication or item of information and does not, once separated, reveal anything of what might reasonably be considered to be the meaning (if any) of any communication or item of information (disregarding any inferred meaning). Examples of such data include:

- the location of a meeting in a calendar appointment;
- photograph information - such as the time/date and location it was taken; and
- contact 'mailto' addresses within a webpage.

[11] Systems data held on a relevant system may be obtained via an equipment interference warrant under Part 5 or Chapter 3 of Part 6 of the Act.

Communications Data Retention Notices

3. Data Retention Notices

3.1. Section 87(1) of the Act gives the Secretary of State the power to give a data retention notice to a telecommunications operator or postal operator, requiring them to retain relevant communications data, if it is considered necessary and proportionate for one or more statutory purposes. Therefore, the default position is that no operator is required to retain any data under the Act until given a notice. Equally, where a notice is given, it must only cover data the retention of which is necessary and proportionate. The statutory purposes for which data can be required to be retained are:

- in the interests of national security;
- for the applicable crime purpose;[12]
- in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose 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; and
- to assist investigations into alleged miscarriages of justice.

3.2. Section 2 of the Act requires the Secretary of State to have regard to the following when giving, varying, or revoking a notice:

- whether what is sought to be achieved by the notice could reasonably be achieved by other less intrusive means;
- whether the level of protection to be applied in relation to obtaining communications data is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems and postal services; and
- any other aspects of the public interest in the protection of privacy.

3.3. Data retained for the purposes set out above can only be accessed by public authorities for those purposes under Part 3 of the Act, where it is necessary and

[12] To the extent that a retention notice relates to events data this is the purpose of preventing or detecting serious crime. To the extent that a retention notice relates to entity data this is the purpose of preventing or detecting crime or of preventing disorder (see paragraph 3.4 within the Communications Data Code of Practice)

proportionate to do so or under other appropriate statutory regimes. The consideration of necessity and proportionality involves balancing the extent of the interference with an individual's right to respect for their private life and, where relevant, with freedom of expression, against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest. Further information on this can be found in Chapter 3 of the Communications Data Code of Practice.

4. Giving of Data Retention Notices

Process for Giving a Data Retention Notice

4.1. The Home Office and key operational agencies (including law enforcement agencies and security and intelligence agencies) maintain governance arrangements in order to identify operational requirements, including the potential requirement to give a data retention notice.

4.2. Once a potential requirement is identified, the Home Office will consult the relevant telecommunications operator(s) or postal operator(s) and, if appropriate, the Secretary of State will consider giving a notice.

Criteria for Issuing a Data Retention Notice

4.3. When considering whether to give a notice a number of factors are taken into account. These include, but are not limited, to:

- The size of the telecommunications operator or postal operator – an operator with a larger customer base is more likely to receive a data retention notice;
- the speed of growth of the telecommunications operator or postal operator – small telecommunications operators or postal operators with rapid prospective growth may receive notices in anticipation of future operational requirements;
- the number of authorisations or notices the telecommunications operator or postal operator receives annually for communications data – this, and the operator's ability to meet the volume of authorisations or notices they receive, will be a key determinant of whether there is benefit in giving a notice to a telecommunications operator or postal operator (noting that the giving of a notice may increase the number of authorisation or notices received by an operator);
- whether the telecommunications operator or postal operator operates a niche service – an operator which is the sole or key provider of a type of service may receive a notice regardless of the size of the company; or
- whether the telecommunications operator or postal operator operates in a specific geographical area – an operator which is a key provider of services in a limited geographical area is more likely to receive a notice.

4.4. Ultimately, however, a notice can only be given where the Secretary of State, having taken into account relevant information, considers it necessary and

proportionate to do so and where the decision to do so has been approved by a Judicial Commissioner.

4.5. The timescale for such processes will depend on operational need but will always follow the same steps to ensure that the Secretary of State is making an informed decision, based on the relevant information.

Third-Party Data

4.6. Where a communication is sent there may be multiple providers involved in the delivery of the communication. Each provider may require different elements of communications data to route the communication. For example, when sending an email there will be the email provider, the internet access provider for the sender and the internet access provider for the recipient. The email provider will require the email address to route the communication but neither internet access provider has any need to see or access the full email address in order to connect the sender or recipient to the mail server.

4.7. Where one telecommunications operator is able to see or access the communications data in relation to applications or services running over their network, in the clear, but does not process that communications data in any way this is regarded as third-party data. A telecommunications operator is considered to process data if it specifically looks at an item of data in order to determine what action to take or if it has a set of rules in place which determine how a communication should be routed depending on certain items of data.

4.8. If a telecommunications operator or postal operator has no need to process data to route a communication but extracts and retains this data or a product generated from this data for their own business purposes, such as for network diagnostics, then this is no longer regarded as third-party data. This data could therefore be covered by a data retention notice.

4.9. Data would not be considered third party-data where it is, or can only be obtained by processing, an internet connection record or where it relates to a relevant roaming service.

4.10. A relevant roaming service exists where a UK telecommunications operator has an international roaming agreement with an overseas telecommunications operator (OTO) which facilitates access to a telecommunications service or services provided by the OTO to one of its customers roaming in the UK. For example, where a person is using a SIM card or eSIM from an OTO to access the OTO's services while roaming on a UK mobile network. In these circumstances, the retention notice could cover retention of communications data by the UK telecommunications operator that relates to the calls and messaging that are handled by the OTO.

4.11. A communications data authorisation may be given for the acquisition by a public authority of third-party data on a forward-looking basis where necessary and proportionate in relation to a specific investigation or operation. A telecommunications operator or postal operator need only obtain and disclose third party data where reasonably practicable to do so. Where such data is encrypted by the third party, a telecommunications operator is under no obligation to decrypt such information solely by virtue of a communications data authorisation.

Criteria for Giving a Notice to Categories of Providers

4.12. There may be circumstances where there are a number of telecommunications operators or postal operators providing similar services in a specific limited area. An example of this could be Wi-Fi providers in a particular location.

4.13. It is possible that the Secretary of State could place the same obligations on all such telecommunications operators or postal operators through one notice, but only if it was considered necessary and proportionate to do so.

4.14. While this may be appropriate for a relatively small number of providers providing the same or a similar service, this provision cannot be used to place blanket requirements across a large number of companies operating a service or companies providing a range of different services, not least because the requirements in a notice need to reflect the particular nature of each business.

Consultation with Operators

4.15. Section 88(2) of the Act requires that before giving a notice to a company the Secretary of State must take reasonable steps to consult any telecommunications operator(s) or postal operator(s) which will be subject to the notice.

4.16. In practice, informal consultation is likely to take place long before a notice is given in order that the operator(s) understands the requirements that may be imposed and can consider the impact. The Government will engage at an early stage with telecommunications operators or postal operators who may be subject to a notice in the future to provide advice and guidance and prepare them for the possibility of receiving a notice.

4.17. In the event that the giving of a notice to a telecommunications operator or postal operator is deemed appropriate, the Secretary of State must take reasonable steps to formally consult the company before giving a notice, in order to ensure that it accurately reflects the services and data types processed by that telecommunications operator or postal operator and to ensure that the telecommunications operator or postal operator understands the obligations

being placed on it, including those in relation to the audit functions of the Information Commissioner. The Secretary of State may delegate participation in this exercise to their officials. In addition to discussion of the matters listed at paragraph 4.21, the formal consultation must also include discussion of the design of any systems to be put in place to give effect to the requirements of the notice.

4.18. Should the telecommunications operator or postal operator have concerns about whether the reasonableness, cost, or technical feasibility of the requirements to be set out in the notice, these should be raised during this formal consultation process. At the conclusion of these discussions, any outstanding concerns must be taken into account by the Secretary of State as part of the decision-making process. Should a telecommunications operator or postal operator continue to have concerns in respect of the feasibility of a notice once given they may refer the notice to the Secretary of State for review (see Chapter 13).

4.19. Should it be considered appropriate to place the same obligations on a number of companies through one notice, the Home Office will take steps to consult all telecommunications operators or postal operators who would or could be affected by the notice. However, it is recognised that there may be cases where this will not be possible, for example where a new telecommunications operator or postal operator enters the market after a notice has been given and therefore will not have been formally consulted. In such circumstances the Secretary of State must take reasonable steps to formally consult any relevant telecommunications operators and postal operators which enter the market after such a notice is given.

Matters to be Considered by the Secretary of State

4.20. Following the conclusion of consultation with a telecommunications operator or postal operator, the Secretary of State will consider whether to give a data retention notice. This decision should include consideration of all the aspects of the proposed data retention notice and its effect on the telecommunications operator or postal operator. It is an essential means of ensuring that the data retention notice is justified and that proper processes have been followed.

4.21. As part of the decision the Secretary of State must take into account a number of factors:

- the likely benefits of the notice in respect of each of the services to which it relates, including the extent to which the data to be retained may be of use to public authorities. This may take into account projected as well as existing benefits and must be in respect of the statutory purposes for which the data can be retained;

- the appropriateness of limiting data to be retained by reference to location or descriptions of persons to whom telecommunications services are provided. These considerations will include determining whether the full geographical reach of the retention notice is necessary and proportionate and whether it is necessary and proportionate to include or exclude any particular descriptions of persons;

- the likely number of users (if known) of the services to be covered by the notice – this will help the Secretary of State to consider both the level of intrusion on customers but also the likely benefits of the data to be retained;

- the technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator(s) or postal operator(s);

- the likely cost of complying with the notice – this will include the costs of both the retention, and any other requirements and restrictions placed on telecommunications operators or postal operators, such as ensuring the security of the retained data. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money;[13] and

- any other effect of the notice on the telecommunications operator or postal operator – again taking into account any representations made by the company.

4.22. The Secretary of State will also consider the contents of the proposed notice, including the data to be retained and the period or periods for which that data is to be retained up to a maximum of 12 months.[14]

4.23. In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision. When giving a notice to an operator based in a country outside the UK, this may include consideration of any requirements or restrictions under the law of that country that may arise when the operator complies with any obligation imposed by a data retention notice. Section 2 of the Act also requires the Secretary of State to give regard to the following when giving, varying, or revoking a notice so far as they are relevant:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means,

[13] See paragraph 4.21 for details of the matters the Secretary of State will consider before issuing a data retention notice.

[14] See paragraphs 4.31 – 4.38 for further information on retention periods.

- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

4.24. When considering the public interest in the integrity and security of telecommunication systems the Secretary of State should consider those systems affected by obligations set out in the notice.

4.25. The Secretary of State may give a notice after considering the points above if they consider that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved.

The Content of a Data Retention Notice

4.26. A notice will set out:

- the services in relation to which data is to be retained – for example, it may not be necessary and proportionate to retain data in relation to all communications services provided by a company;
- the data to be retained and the period for which it is retained – these will relate to the categories of data listed as 'relevant communications data'[15] in section 87(11) of the Act and will make clear how long certain categories of data should be retained for;[16] and
- any additional requirements or restrictions in relation to the retention of the data – this may include requirements in relation to the security, integrity, and destruction of retained data and the audit of the telecommunications operator's or postal operator's compliance with these requirements by the Information Commissioner.

4.27. A notice will not necessarily represent the full range of services and data types which a telecommunications operator or postal operator could retain. This does not mean that additional data types or services could not be included in a future version of the notice, should an operational requirement arise, provided that it would be necessary and proportionate to do so (see Chapter 13 for further details).

4.28. Requirements or restrictions in relation to the retention of the data may include:

- a requirement to take such steps as are necessary to ensure that data which is generated and processed by the telecommunications operator or postal

[15] See Chapter 2, 'Scope and Definitions', of the Communications Data Code of Practice.

[16] The data to be retained must be covered in sufficient detail that the telecommunications operator or postal operator is clear exactly what it must retain.

operator (including transitory information in the core systems) is made available to be retained;

- a requirement to process the data to ensure that multiple items of data from a single system or multiple systems within an operator can be stored in a single clear record where appropriate to do so. This will ensure the volume of data retained is limited to that which is truly necessary; or

- a requirement to test the viability of retaining certain data or developing a retention system over a phased timescale.

Generation and Processing of Data

4.29. A retention notice may also include requirements in relation to the generation and processing of retained data. Such requirements may include:

- a requirement to retain data in such a way that it can be transmitted efficiently and effectively in response to authorisations and notices (including linking events to user accounts);

- a requirement to process the data to ensure that multiple items of data from a single or multiple systems within an operator can be stored in a single clear record where appropriate to do so;

- a requirement to filter the data to remove records that are not of interest, including duplicate events or where aggregated records or summaries have been created; and

- a requirement to generate data that relates to a relevant roaming service or for the processing of an internet connection record (see paragraph 4.10).

4.30. Aggregation, summarising, and filtering of data will ensure the volume of data retained is limited to that which is truly necessary.

Retention Period

4.31. Data retained under the Act may be retained for a maximum of 12 months.

4.32. A notice will only require data to be retained for as long as is considered necessary and proportionate, up to that maximum period. If, once a data retention notice is given, further evidence demonstrates that a retention period specified in the notice is no longer appropriate, the Secretary of State will set a different retention period, up to a maximum of 12 months, ensuring the period reflects what is necessary and proportionate.

4.33. A data retention notice may cover data already in existence at the point at which a notice is given or it may require the generation of data.

4.34. The starting point for the retention period for data in existence at the point of the notice is determined by the type of data.

4.35. The retention period for a specific communication commences on the day of the communication concerned. Some internet communications, such as broadband sessions, may remain active for days, or even months. In such cases the retention period commences on the day on which the communication ends.

4.36. For retained data held by a telecommunications operator or postal operator about an entity to whom a service is provided the retention period commences on the day on which the entity concerned ceases to be connected to the service or if the data is changed. For example, previous addresses for a customer may only be retained for a maximum of 12 months after the telecommunications operator or postal operator changes the data in their systems, irrespective of whether the customer remains with the service.

4.37. For all other communications data held by a telecommunications operator or postal operator, including where data is required to be generated, then the retention period will start from the moment the data comes into existence.

4.38. Sometimes a telecommunications operator or postal operator may already retain data for 12 months or more for business purposes. Such data may still be subject to a retention notice to ensure that the data is available with the maximum 12-month period in case the business need for the data changes and the telecommunications operator or postal operator decides to delete the data.

5. Security, Integrity, and Destruction of Retained Data

5.1. All data retained under the Act is subject to a range of safeguards in order to ensure effective protection of the data against the risk of abuse and any unlawful access to and use of that data. Section 92 of the Act requires telecommunications operators and postal operators under a notice to take steps to ensure that the data is adequately protected while it is being retained. Importantly, that section requires that data must be of the same integrity and at least of the same security as the system from which it has been derived. Requirements beyond that minimum standard relate to three broad areas – data security, data integrity and destruction of data.

5.2. Further detail on the security arrangements to be put in place by telecommunications operators and postal operators may be included in the data retention notice given to a telecommunications operator or postal operator which, in accordance with section 87(8)(d), must specify any other requirements or restriction in relation to the retention of data.

5.3. In most cases data retained under a notice is stored in a dedicated data retention system, which is securely separated by technical security measures (e.g., a firewall) from a telecommunications operator's or postal operator's business system. Where data is retained by telecommunications operators or postal operators for business purposes for some, but not all, of the period specified in the notice, the data retention system may hold a duplicate of that business data so that it can be accessed efficiently and effectively.

5.4. However, in some cases it will not be practical to create a duplicate of that data and telecommunications operators or postal operators will retain information in business or shared systems.

5.5. The scope of the security controls defined within this section apply to all systems where data is retained by virtue of a retention notice. The security controls also include any other systems which are used to access, support, or manage data retained under a retention notice. The security controls also apply to all telecommunications operator or postal operator (or third party) operational and support staff who have access to such systems. Additional security considerations may be required to enable systems for the disclosure of communications data to connect securely to acquisition systems in public authorities.

5.6. Where data is retained in business or shared systems, or where business systems are used to access, support, or manage systems containing data retained by virtue of a retention notice, these will be subject to specific security

controls and safeguards, similar to those defined within this section, where appropriate and as agreed with the Home Office.

5.7. Where data was originally retained by virtue of a retention notice, but it has subsequently been moved or copied by the telecommunications operator or postal operator into another system, the security controls in the Act and this code do not apply. This is because the scope of these security controls can only apply insofar as they relate to data retained by virtue of a retention notice. However, any processes or systems that are involved in the transferring or copying of data retained under a retention notice into another system are subject to these security controls.

Data Security

5.8. The specific data security measures required by a telecommunications operator or postal operator to protect retained data will depend on a number of factors including, but not limited to, the volume of data being retained, the number of customers whose data is being retained and the nature of the retained data.

5.9. When setting security standards consideration must also be given to the threat to the data.

5.10. The security put in place at a telecommunications operator or postal operator will comprise four key areas:

- physical security controls e.g., buildings, server cages, CCTV;
- technical security controls e.g., firewalls and anti-virus software;
- personnel security controls e.g., staff security clearances and training; and
- procedural security e.g., processes and policies.

5.11. As each of these broad areas is complementary, the balance between these may vary e.g., a telecommunications operator or postal operator that is able to provide less rigorous personnel security control outcomes may require more comprehensive technical and procedural security controls to be put in place. The specific security arrangements put in place will be agreed in confidence between the Home Office and relevant telecommunications operators or postal operators and shared with the Information Commissioner for the purposes of his functions under this code.

5.12. The level of data security is based on a number of factors and is a balance of these four broad areas. All telecommunications operators and postal operators retaining data will be required to follow the key principles of data security set out in paragraphs 5.19 to 5.54. It is open to a telecommunications operator or

postal operator to put in place alternative controls or mitigations which provide assurance of the security of the data, where agreed with the Home Office.

5.13. The Home Office will provide security advice and guidance to all telecommunications operators and postal operators who are retaining data and this will also be provided to the Information Commissioner for the conduct of their functions under this code.

Data Integrity

5.14. Data integrity, as required by section 92(1)(a), relates to a need to ensure that no inaccuracies are introduced to data when it is retained under the Act and that the data is not altered.[17]

5.15. When relevant communications data is retained under the Act, it should be a faithful reproduction of the relevant business data[18] and it should remain a faithful reproduction throughout any further processing that may occur during the period of its retention. A record of the business purpose for which the data is generated may be retained to assist law enforcement to understand the underlying quality and completeness of the business data which has then been retained. For example, data generated to assist a telecommunications operator or postal operator in understanding network loading may be less accurate than data used to bill customers.

5.16. There should be no errors introduced in retaining the data, for example in the process of copying the data to a retained data store or in searching and disclosing data, that lead to discrepancies between the business and retention sets of data.

5.17. Once the data has been retained, technical security controls should be implemented to mitigate modification of the data, and to audit any attempt to modify the data, until such time that it is deleted in accordance with section 92(2) of the Act.

5.18. The audit capability of the data retention system should be used to provide assurance that no unauthorised changes have been made to the retained data.

[17] This includes at the point at which it is placed into a data retention system and during the period of its retention.

[18] Where data is generated in relation to requirements set out in a data retention notice, it should be a faithful reproduction of relevant business data and/or the relevant network data.

Principles of Data Security, Integrity, and Destruction

Legal and Regulatory Compliance

5.19. All data retention and disclosure systems and practices must be compliant with relevant legislation. As well as the Act, this includes relevant data protection legislation, which sets out key controls in relation to the storage, use and transfer of personal data.

5.20. All systems and practices must also comply with any security policies and standards in place in relation to the retention of communications data. This may include any policies and standards issued by the Home Office, and any instruction or recommendation made by the Information Commissioner such as published guidance on security. Further requirements are unlikely to be publicly available where they contain specific details of security infrastructure or practices, disclosure of which could create additional security risks.

Information Security Policy and Risk Management

5.21. Each telecommunications operator or postal operator in receipt of a data retention notice must develop a security policy document. The policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities and policies relating to the integrity and destruction of data. Each telecommunications operator or postal operator must also develop security operating procedures, including clear desk and screen policies for all systems. A telecommunications operator or postal operator can determine whether this forms part of or is additional to wider company policies.

5.22. The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate to the nature of the business, the data retained and the threats to data security.

5.23. Each telecommunications operator or postal operator must identify, assess and treat all information security risks, including those which relate to arrangements with external parties.

Human Resources Security

5.24. Telecommunications operators and postal operators must clearly identify roles and responsibilities of staff and contractors (personnel), ensuring that roles are appropriately segregated to ensure staff only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when personnel move roles within the organisation.

5.25. Personnel with access to the data retention systems should be subject to an appropriate level of security screening. The Government sponsors and

manages security clearance for certain personnel working within telecommunications operators and postal operators. Telecommunications operators and postal operators must ensure that these personnel have undergone relevant security training and have access to security awareness information.

Maintenance of physical security

5.26. Data retention systems should have appropriate security controls in place. Access to the locations where the systems are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

5.27. Equipment used to retain data must be sanitised and securely disposed of at the end of its life (see the section on destruction of data beginning at paragraph 5.43).

Operations Management

5.28. Data retention systems should be subject to a documented change management process, including changes to third party suppliers, to ensure that no changes are made to systems without assessing the impact on the security of retained data.

5.29. Telecommunications operators and postal operators must also put in place a patching policy to ensure that regular patches and updates are applied to any data retention system as appropriate. Such patches and updates will include anti-virus, operating systems, application, and firmware. The patching policy, including the timescale in which patches must be applied, must be agreed with the Home Office.

5.30. Telecommunications operators and postal operators should ensure that, where encryption is in place in data retention systems, any encryption keys are subject to appropriate controls, in accordance with the security policy.

5.31. In order to maintain the integrity of internal data processing telecommunications operators and postal operators must ensure that data being processed is validated against agreed data security criteria.

5.32. Network infrastructure, services and system documentation must be secured and managed and an inventory of all assets should be maintained together with a clear identification of their value and ownership. All assets must be clearly labelled.

5.33. Telecommunications operators and postal operators should also ensure that removable and storage media (including the hard drives used to store retained data) are managed in accordance with the security policy, especially when in transit.

5.34. The data retention system, and its use, should be monitored and all audit logs compiled, secured, and reviewed by the telecommunications operator's or postal operator's security manager at appropriate intervals. These should be made available for inspection by the Home Office as required.

5.35. Telecommunications operators and postal operators should ensure that systems are resilient to failure and data loss by creating regular back-ups of the data.

5.36. Technical vulnerabilities must be identified and assessed through an independent IT Health Check which must be conducted annually. The scope of the Health Check must be agreed with the Home Office.

Access Controls

5.37. Telecommunications operators and postal operators must ensure that registration and access rights, passwords, and privileges for access to dedicated data retention systems are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

5.38. Access to operating systems must be locked down to an appropriate standard and any mobile computing (i.e., offsite access to telecommunications operator or postal operator systems from non-secure locations) must be subject to appropriate policies and procedures if permitted. Accordingly, any remote access for diagnostic, configuration and support purposes must be controlled.

5.39. Access should be provided to relevant oversight bodies where necessary for them to carry out their functions.

Management of Incidents

5.40. Telecommunications operators and postal operators must put in place clear incident management processes and procedures, including an escalation path to raise issues to senior management and the Home Office. Any breaches under relevant legislation, should be notified in accordance with those provisions.

5.41. Measures should be implemented to prevent unauthorised disclosure or processing of data. Any suspected or actual unauthorised disclosure or processing of data or information must be reported as set out above.

5.42. System managers must ensure that data retention systems enable the collection of evidence (e.g., audit records) to support investigation into any breach of security.

Additional Requirements relating to the Destruction of Data

5.43. Section 92(2) of the Act makes clear that retained data must be destroyed[19] such that it is impossible to access at the end of the period for which it is required to be retained, unless its retention is otherwise authorised by law. A system must be set up such that it is verifiable that data is deleted and inaccessible at the end of the retention period. Deletions must take place at intervals no greater than monthly. However, telecommunications operators and postal operators should strive to delete data as soon as practically and technically possible at the end of the retention period. If investigators are seeking data that they know may be close to the end of the retention period, SPoCs (single points of contact) should liaise with telecommunications operators and postal operators to see whether any steps can be taken to expedite the request.

5.44. Crypto-shredding (also referred to as Cryptographic Erasure) can be used as an acceptable alternative where data overwriting, or physical destruction of storage media cannot be verified, or is not feasible, such as in cloud environments. Telecommunications operators and postal operators must ensure that:

- All encryption keys are generated, stored, and zeroised (deleted) on premises (i.e., outside of the cloud service provider, or any third-party environment).

- All key management practises are documented and auditable if required by the Home Office.

5.45. To prevent future key compromise and/or data reidentification, telecommunications operators and postal operators must ensure strong cryptographic algorithms and modes of operation are used in the generation of all cryptographic keys in compliance with industry standards.

5.46. Telecommunications operators and postal operators must ensure that the cloud service provider can support the data retention, security, and destruction requirements of communications data, set out in this code of practice.

5.47. In the case of data not stored in a cloud environment, where the physical, personnel and procedural security measures are assessed by the Home Office (or Information Commissioner) to be sufficient to prevent unauthorised physical access to the data retention system, then data should be deleted in such a way that protects against data recovery using non-invasive attacks (i.e. attempts to retrieve data without additional assistance from physical equipment).

5.48. Where the implemented security measures are assessed by the Home Office (or Information Commissioner) to be insufficient to protect the data retention

[19] Section 263(1) of the Act defines ‘destroy’ for the purposes of the Act to mean ‘delete the data in such a way as to make access to the data impossible.

system against physical access by unauthorised personnel, then additional requirements for the secure destruction of retained data should be agreed with the Home Office and Information Commissioner on a case-by-case basis.

Additional Requirements relating to the Disposal of Systems

5.49. The legal requirement to ensure deleted data is unviable to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

5.50. If the equipment is to be re-used and it is not stored in a cloud environment, it must be securely sanitised by means of overwriting using a government approved product. In the case of data stored in a cloud environment, it must be destroyed via crypto-shredding as per paragraphs 5.44 - 5.46. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

5.51. If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction.

5.52. Sanitisation or destruction of data must include retained data copied for back-up and recovery, and anything else that stores duplicate data within the telecommunications operator and postal operator system, unless retention of the data is otherwise authorised by law.

Location of Retained Data

5.53. The location of retained data will be relevant to the security of the data but is only one of a number of factors which are relevant – such as the specific technical security protections. Ensuring the data is retained securely is more important than a general requirement on where the data must be retained that does not take account of specific circumstances.

5.54. The principles of only transferring data when it is consistent with data protection requirements and ensuring the data is retained to an appropriate level of security will apply.

6. Disclosure and the Use of Data

Disclosure of Data

6.1. As per section 93 of the Act, a telecommunications operator or postal operator must put in place adequate security systems (including technical and organisational measures) governing access to retained communications data in order to protect against any unlawful disclosure.

6.2. Section 87(9)(a) of the Act clarifies that telecommunications operators and postal operators can be required to retain data in such a way that it can be transmitted efficiently and effectively in response to requests for communications data. In such circumstances, the Home Office will work with telecommunications operators and postal operators to ensure that the necessary secure auditable systems are in place to enable this disclosure.[20]

6.3. The main purpose of retaining relevant communications data is to make that data available, where necessary and proportionate, for disclosure under Part 3 of the Act. However, there may be other circumstances in which telecommunications operators and postal operators may lawfully disclose retained communications data. Such circumstances could include:

- requests from an emergency service for data in relation to an emergency call (Chapter 10 of the Communications Data Code of Practice);
- requests for personal data held by a company via a subject access request under relevant data protection legislation;[21]
- where a telecommunications operator or postal operator proactively discloses communications data to relevant public authorities or regulatory bodies such as in cases of suspected criminality.

Use of Data by Telecommunications Operators and Postal Operators

6.4. If data is held subject to a notice and would not otherwise be held by the telecommunications operator or postal operator for business purposes, it should be adequately safeguarded to ensure that it can only be accessed for purposes connected to that notice. If data is not also being retained for existing business purposes it cannot be used by telecommunications operators and postal

[20] Requiring telecommunications or postal operators to retain communications data in such a way that the data can be transmitted efficiently and effectively in response to requests may include specifying expected response times to requests.

[21] See paragraph 12.13 onwards within the Communication Data Code of Practice.

operators for business purposes without permission from the Home Office. Home Office permission would not be given for matters such as marketing. However, there may be some circumstances where it could be considered in the public interest for the telecommunications operator or postal operator to access the retained data. For example, if a customer is receiving malicious calls or if a telecommunications operator or postal operator identifies suspected criminality on the network. Home Office agreement for the telecommunications operator or postal operator to access the retained data in such circumstances may relate to individual requests or categories of request.

Technical Capability Notices

7. Technical Capability Notices

7.1. Telecommunications operators or postal operators may be required under section 253 of the Act to have the capability to provide assistance in giving effect to interception, equipment interference and bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice is served, companies can give effect to it securely and quickly.

7.2. The Secretary of State may give a relevant telecommunications operator or postal operator a technical capability notice imposing on the relevant operator obligations that are specified in regulations made by the Secretary of State and set out on the notice, and requiring the person to take all steps specified in the notice. The Secretary of State may only give a notice where the decision to do so has been approved by a Judicial Commissioner. In practice, technical capability notices are likely only to be given to telecommunications operators and postal operators required to give effect to relevant authorisations (i.e., warrants served under Parts 2, 5 or 6 of the Act, or authorisations and notices given under Part 3 of the Act) on a recurrent basis.

7.3. Small companies (providing or intending to provide a telecommunications service to fewer than 10,000 persons) will not be given a notice obligating them to provide and them to have capacity to provide assistance in giving effect to an interception or equipment interference capability, although they may be required to give effect to a warrant.

7.4. In the event that a number of telecommunications operators are involved in the provision of a service, the obligation(s) will be placed on the telecommunications operator which is able to give effect to the notice and on whom it is necessary and proportionate to impose the requirements. It is possible that more than one telecommunications operator will be involved in the provision of the capability. In such circumstances, it is likely to be necessary for the operator to whom the notice is given to disclose, with the permission of the Secretary of State, the existence of the notice (see paragraphs 10.16 - 10.19). The only obligations that may be imposed by a technical capability notice are those set out in regulations made by the Secretary of State and approved by Parliament. Before making these regulations, the Secretary of State must consult the Technical Advisory Board, telecommunications operators or postal operators appearing to the Secretary of State to be likely to be subject to obligations specified in the regulations, persons representing operators and persons with statutory functions in relation to operators, including the Investigatory Powers Commissioner.

7.5. Section 253(4) provides that the obligations that the Secretary of State may include in regulations, and thus which may be imposed on operators, must be reasonable for the purpose of securing that it is (and remains) practicable to impose requirements on a relevant operator, and that it is practicable for the operator to comply with those requirements. For example, an obligation relating to the security of a telecommunications service or telecommunication system can be imposed by a technical capability notice for the purpose of ensuring that the operator has the capability to assist in giving effect to an interception warrant in such a manner that the risk of any unauthorised persons becoming aware of the existence of the warrant is minimised. Section 253(5) gives examples of the sorts of obligations that such regulations may include:

- obligations to provide facilities or services of a specified description;
- obligations relating to apparatus owned or operated by a relevant operator;
- obligations relating to the removal of electronic protection applied by or on behalf of the relevant operator on whom the obligation has been placed to any communications or data;
- obligations relating to the security of any postal or telecommunications services provided by the relevant operator; or
- obligations relating to the handling or disclosure of any content or data.

7.6. An obligation imposed by a technical capability notice on a telecommunications operator to remove encryption does not require the operator to remove encryption per se. Rather, it may require that operator to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation.

7.7. As with any other obligation contained in a technical capability notice, an obligation to remove encryption may only be imposed where it is reasonably practicable for the relevant telecommunications operator to comply with it. A decision regarding what is reasonably practicable will depend on the particular circumstances of the case, recognising that what is reasonably practicable for one telecommunications operator may not be for another. Such an obligation may only relate to electronic protections that the company has itself applied to communications or data, or where those protections have been applied on behalf of that telecommunications operator, and not to encryption applied by any other party. References to protections applied on behalf of the telecommunications operator include circumstances where the operator has contracted a third party to apply electronic protections to a telecommunications service offered by that telecommunications operator to its customers.

7.8. While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, a warrant may require a telecommunications operator to take such steps as are reasonably practicable to take to give effect to it. This will include, where applicable, providing communications or data in an intelligible form. An example of such circumstances might be where a telecommunications operator removes encryption from communications or data for their own business reasons.

Consultation with Operators

7.9. Before giving a notice, the Secretary of State must consult the telecommunications operator or postal operator.[22] In practice, informal consultation is likely to take place long before a notice is given in order that the operator understands the requirements which may be imposed and can consider their impact. The Secretary of State's representatives, which includes intelligence agency staff and the National Technical Assistance Centre (NTAC), will engage at an early stage with telecommunications operators or postal operators who are likely to be subject to a notice in order to provide advice and guidance, and prepare them for the possibility of receiving a notice.

7.10. In the event that the giving of a notice to a telecommunications operator or postal operator is deemed appropriate, the Secretary of State must consult the telecommunications operator or postal operator before the notice is given. The Secretary of State may delegate participation in this exercise to their officials. In addition to discussion of the matters listed at 7.13, the consultation must also include discussion of the design of any technical capability to be used to give effect to warrants. This will ensure that any capability will meet the requirements of the notice prior to development.

7.11. Should the telecommunications operator or postal operator have concerns about the reasonableness, cost, or technical feasibility of the obligations to be set out in the notice, these should be raised during the consultation process. At the conclusion of these discussions, any outstanding concerns must be taken into account by the Secretary of State as part of the decision-making process.

Matters to be Considered by the Secretary of State

7.12. Following the conclusion of consultation with a telecommunications operator or postal operator, the Secretary of State will decide whether to give a notice. This decision should include consideration of all the aspects of the proposed notice and its effect on the telecommunications operator or postal operator. It is an

[22] See section 255(2) of the Act.

essential means of ensuring that the notice is necessary and proportionate to what is sought to be achieved, and that proper processes have been followed.

7.13. As part of the decision, the Secretary of State must take into account, amongst other factors, the matters specified in section 255(3):

- the likely benefits of the notice – this may take into account projected as well as existing benefits;
- the likely number of users (if known) of any postal or telecommunications service to which the notice relates – this will help the Secretary of State to consider both the necessity of the capability but also the likely benefits;
- the technical feasibility of complying with the notice – taking into account any representations made by the telecommunications operator or postal operator and giving specific consideration to any obligations in the notice to remove electronic protections (as described at section 255(4));
- the likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator or postal operator as part of the notice, such as those relating to security. This should also include specific consideration to the likely cost of complying with any obligations in the notice to remove electronic protections. This will enable the Secretary of State to consider whether the imposition of a notice is affordable and represents value for money; and
- any other effect of the notice on the telecommunications operator or postal operator – again taking into account any representations made by the company.

7.14. In addition to the points above, the Secretary of State should consider any other issue which is relevant to the decision. When giving a notice to an operator based in a country outside the UK, this may include consideration of any requirements or restrictions under the law of that country that may arise when the operator complies with any obligation imposed by a technical capability notice, or when the operator provides subsequent assistance in relation to a warrant or other relevant authorisation. Section 2 of the Act also requires the Secretary of State to have regard to the following when giving, varying, or revoking a notice so far as they are relevant:

- whether what is sought to be achieved by the notice could reasonably be achieved by other less intrusive means;
- the public interest in the integrity and security of telecommunication systems and postal services; and
- any other aspects of the public interest in the protection of privacy.

7.15. When considering the public interest in the integrity and security of telecommunication systems the Secretary of State should consider those systems affected by obligations set out in the notice, with particular reference to any obligations relating to the removal of encryption.

7.16. The Secretary of State may give a notice after considering the points above if he or she considers that the notice is necessary, and that the conduct required is proportionate to what is sought to be achieved. The obligations set out in the notice must be limited to those set out in regulations made by the Secretary of State under section 253, as described above.

7.17. Before the notice may be given, a Judicial Commissioner must approve the Secretary of State's decision to give the notice. In deciding whether to approve the Secretary of State's decision to give a relevant notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the notice is necessary and whether the conduct it requires is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2.

8. Security, Integrity, and Disposal of Interception Capabilities, Equipment Interference Systems, and Retained Data

8.1. The only obligations that may be imposed by a technical capability notice, including security requirements, are those detailed in regulations made by the Secretary of State and approved by Parliament. These obligations are set out in The Investigatory Powers (Technical Capability) Regulations 2018.[23] A technical capability notice will set out which of these obligations apply to the operator to whom the notice will be given, and may detail how these requirements should be affected.

8.2. The regulations require telecommunications operators and postal operators to ensure that apparatus, systems, or other facilities or services, as well as procedures and policies (including on physical, document, operational and non-operational information technology, and personnel security), are developed and maintained in accordance with standards or guidance as specified in the notice. In the case of interception this will also be subject to guidance, as provided by NTAC. Such obligations may include implementing guidance on information security, as provided by the National Cyber Security Centre.[24]

8.3. A decision regarding what security obligations are reasonably practicable to impose on an operator will depend on the particular systems and processes already in place. A decision must therefore be made on a case-by-case basis, recognising that one model is unlikely to be appropriate for all operators.

Data Security

8.4. The following sections provide detail of the security requirements which are likely to be imposed by a technical capability notice. The security requirements imposed on a telecommunications operator or postal operator, required to protect interception capabilities and interception product, will comprise four key areas:

- physical security controls e.g., buildings, server cages, CCTV;

[23] The Investigatory Powers (Technical Capability) Regulations 2018 (legislation.gov.uk) – SI/2018/353 – https://www.legislation.gov.uk/uksi/2018/353/made

[24] For further details, please see guidance on the National Cyber Security Centre's website: www.ncsc.gov.uk.

- technical security controls e.g., firewalls and anti-virus software;
- personnel security controls e.g., staff security clearances and training; and
- procedural security controls e.g., processes and policies.

8.5. As each of these broad areas is complementary, the balance between these may vary e.g., a telecommunications operator that is able to achieve less rigorous personnel security control outcomes may require more comprehensive technical and procedural security controls to be put in place.

8.6. The specific security arrangements put in place to ensure compliance with the notice will be agreed in confidence between the Secretary of State and the relevant telecommunications operator or postal operator. In practice, the Secretary of State can delegate completion of elements of this activity to officials, although the final decision to sign and issue the notice will always be made by the Secretary of State. As the overall level of security control is based on the specific circumstances of the telecommunications operator or postal operator which receives a technical capability notices, and is likely to require a balance of four broad areas described above, there is no single security standard. However, all telecommunications operators and postal operators in receipt of a technical capability notice will be required to follow the key principles of security set out in paragraphs 8.18 to 8.61 (Principles of data security, integrity, and disposal of systems).

8.7. A telecommunications operator or postal operator may be permitted to implement alternative security controls or risk mitigations to those initial specified in a technical capability notice if they can evidence that these provide equivalent protection and assurance of the security of the relevant technical capabilities and data, and where this change has been agreed with the Secretary of State, their officials, and – when in relation to interception – NTAC. The Home Office will provide security advice and guidance to all telecommunications operators and postal operators who are retaining data, and this will also be provided to the Information Commissioner for the conduct of his functions under this code.

8.8. In the case of interception capabilities and products, telecommunications operators and postal operators operating under technical capability notices will provide timely access to NTAC to assess physical, personnel, procedural and technical security. NTAC will provide subsequent security advice and guidance to the telecommunications operator or postal operator.

Security Arrangements relating to Interception Capabilities and Products

8.9. Specific security requirements will relate to a number of broad areas – the interception capabilities, the security and integrity of interception factors, the delivery of intercepted material, and the secure destruction of interception identifiers/factors.

8.10. A Service Level Agreement may also be negotiated between the Secretary of State and the telecommunications operator or postal operator. If agreed, this document will provide details of how the obligations imposed by a technical capability notice will be implemented and maintained, including those that relate to security.

8.11. The scope of the security controls defined within this section apply to all dedicated IT systems that are used to access, support or manage dedicated interception systems. It also applies to all operator (or third party) operational and support staff who have access to such systems.

8.12. Systems holding intercepted material will be securely separated by technical security measures (e.g., a firewall) from a telecommunications operator's or postal operator's business systems. However, interception capabilities may make use of equipment currently in place at the operator's facilities.

8.13. Where interception factors are retained in business or shared systems, or where business systems are used to access, support, or manage interception capabilities, these will be subject to specific security controls and safeguards as considered appropriate by the Secretary of State.

Integrity of Interception and Delivered Product

8.14. When interception is authorised and conducted by virtue of a warrant in the Act, checks should be undertaken by the telecommunications operator or postal operator at intervals agreed with NTAC to ensure the integrity and security of interception and the delivery of correct product.

8.15. The intercepting authority must be notified of any errors in the interception. NTAC should be notified of any problems or changes to interception capability or the delivery of intercept product.

8.16. A technical capability notice may require a telecommunications operator or postal operator to ensure that audit systems are in place to provide assurance that no unauthorised changes have been made to the interception identifiers/factors and to confirm details of those identifiers/factors.

8.17. In the event that checks indicate any problems or changes in relation to the warranted interception, the intercepting authority will advise the telecommunications operator or postal operator on any further action that may be required.

Principles of data security, integrity, and disposal of systems

Legal and regulatory compliance

8.18. All interception, equipment interference, and communications data disclosure systems and practices must be compliant with relevant legislation. In the case of communications data disclosure, this includes relevant data protection legislation, which sets out key controls in relation to the storage, use and transfer of personal data.

8.19. All systems and practices must comply with any security policies and standards in place in relation to the interception of communications, equipment interference, and the disclosure of communications data. This may include any policies and standards issued by the Secretary of State or NTAC. These further requirements are unlikely to be publicly available, as they may contain specific details of security infrastructure or practices, the disclosure of which could create security risks.

Information security policy and risk management

8.20. A technical capability notice may require each telecommunications operator and postal operator to whom a notice is given to develop a security policy. In the case of a notice relating to equipment interference systems and practice, the development of a security policy will always be a requirement.

8.21. This policy document should describe the internal security organisation, the governance and authorisation processes, access controls, necessary training, the allocation of security responsibilities, and policies relating to the security and integrity of interception capabilities and information related to warranted interception. Each telecommunications operator and postal operator to whom a notice is given must also develop security operating procedures. An operator can determine whether this forms part of, or is additional to, wider company policies.

8.22. The security policy document and security operating procedures should be reviewed regularly to ensure they remain appropriate.

8.23. A technical capability notice may require each telecommunications operator and postal operator to whom a notice is given to identify, assess, and address all information security risks, including those which relate to arrangements with external parties.

Personnel security

8.24. Telecommunications operators and postal operators must clearly identify roles and responsibilities of staff and contractors (personnel) involved in the provision of assistance to intelligence services and intercepting authorities, ensuring that roles are appropriately segregated to ensure personnel only have access to the information necessary to complete their role. Access rights and permissions assigned to users must be revoked on termination of their employment. Such rights and permissions must be reviewed and, if appropriate, amended or revoked when personnel move roles within the organisation.

8.25. A technical capability notice may require telecommunications operators' and postal operators' personnel with access to equipment interference, capabilities, interception capabilities, sensitive information related to warranted interception, or access to data retention systems to be subject to an appropriate level of security vetting. The Government sponsors and manages security clearance for certain personnel working within a telecommunications operator or postal operator to ensure the company's compliance with obligations under the Act.

8.26. Telecommunications operators and postal operators to whom a notice is given must ensure that these personnel have undergone relevant and regular security training and have access to relevant security awareness information.

8.27. All persons who may have access to intercepted communication or secondary data, the product of equipment interference, communications data, or need to see any reporting in relation to it, must be appropriately vetted. To maintain security clearance, the individual has a responsibility to declare relevant changes in their personal circumstances. Managers should ensure that any changes in circumstances of personnel or behaviours which may indicate a potential security risk are reported. Managers must identify to the Home Office any concerns that may lead to the security clearance of individual members of personnel being reconsidered. The vetting of each individual member of personnel must also be periodically reviewed in line with current HMG security clearance guidance.[25]

8.28. Where it is necessary for an officer of an intercepting authority or a member of NTAC staff to disclose information related to warranted interception to a telecommunications operator or postal operator operating under a technical capability notice, it is the former's responsibility to ensure that the recipient has the necessary security clearance.

[25] UKSV National Security Vetting Solution: guidance for sponsors - GOV.UK (www.gov.uk); https://www.gov.uk/government/publications/uksv-national-security-vetting-solution-portal-guidance-for-sponsors

Maintenance of Physical Security

8.29. A technical capability notice may require there to be appropriate physical security controls in place to prevent unauthorised access to sensitive information. Access to locations where relevant technical capabilities and systems – and associated documentation – are both operated and hosted must be controlled such that access is limited to those with the relevant security clearance and permissions.

8.30. A technical capability notice may require equipment used to intercept communications, retain data, and systems used for the purpose of warranted equipment interference to be sanitised and securely disposed of at the end of its life in accordance with HMG policies.[26]

Operations management

8.31. A technical capability notice may require interception capabilities, data retention systems, and systems used for interference capabilities to be subject to a documented change management process, including proposed changes to third party suppliers, to ensure that no changes are made to systems without prior assessment of the impact on the integrity and security of the product.

8.32. A technical capability notice may require telecommunications operators and postal operators to whom a notice is given to put in place a documented patching policy to ensure that regular patches and updates are applied to any interception capabilities, equipment interference capabilities, data retention system, or support systems as appropriate. Such patches and updates will include anti-virus, operating systems, application, and firmware. The patching policy, including the timescale in which patches must be applied, must be agreed with the Secretary of State – and, in the case of interception, NTAC – during the consultation stage before a notice is given.

8.33. A technical capability notice may require telecommunications operators and postal operators to ensure that, where encryption is in place within interception capabilities and systems, any encryption keys are subject to appropriate management controls, in accordance with the appropriate security policy.

8.34. With regards to interception and data retention, in order to maintain the integrity and security of interception and the delivery of product, telecommunications operators and postal operators must ensure that data being processed is validated against data security criteria, agreed with the Secretary of State and, where appropriate, NTAC during the consultation stage before a notice is given.

8.35. Network infrastructure, services, media, and system documentation must be stored and managed in accordance with the agreed security policy and an inventory of all assets should be maintained together with a clear identification

[26] Please see 8.57 for further details on the disposal of interception systems.

of their value and ownership. All assets must be clearly labelled and regularly accounted for.

8.36. In respect of communications data, telecommunications operators and postal operators should also ensure that removable and storage media (including the hard drives used to store retained data) are managed in accordance with the agreed security policy, especially when in transit.

8.37. Interception and data retention capabilities, and their use, must be monitored and all audit logs compiled, secured, and reviewed by the telecommunications operator or postal operator security manager at appropriate intervals. These should be retained for the period agreed within the security policy and made available for inspection by the Home Office and NTAC as required. In the case of interception capabilities, telecommunications operators and postal operators must demonstrate audit and compliance procedures in line with the requirements set out in their notice. A notice may, for example, require adherence to standards such as ISO27000.

8.38. Telecommunications operators and postal operators should ensure that systems are resilient to risks of technical failure and/or data loss by creating and securely retaining regular back-ups of the data.

8.39. A technical capability notice related to interception and data retention capabilities may require technical vulnerabilities to be identified and assessed through an independent IT Health Check (ITHC) which must be conducted regularly, at an interval set out in the operator's technical capability notice. For interception capabilities, the scope of the ITHC must be agreed with NTAC. Any ITHC undertaken without prior agreement of scope from NTAC will not be considered valid.

Access Controls

8.40. Telecommunications operators and postal operators to whom a notice is given that have access to any equipment that forms part of a technical capability, must ensure that registration and access rights, passwords, and privileges for access to dedicated interception, equipment interference, and data retention systems, and associated documentation are managed in accordance with their security policy. They must also ensure that users understand and formally acknowledge their security responsibilities.

8.41. Access to hypervisors, virtualisation, containerisation, and operating systems must be locked down to an appropriate standard and any mobile computing (i.e., offsite access to a telecommunications operator's systems from non-secure locations) must be subject to appropriate policies and procedures, if permitted. Accordingly, any remote access for diagnostic, configuration and support purposes must be controlled and granted under the principles of least privilege.

8.42. Access should be provided to relevant oversight bodies, where necessary, for them to carry out their functions.

Management of incidents

8.43. A technical capability notice may require telecommunications operators and postal operators in receipt of a technical capability notice to put in place clear incident management processes and procedures, including an escalation path to raise issues to senior management, the Home Office and, where appropriate, NTAC. Any breaches under relevant legislation should be notified in accordance with those provisions. In addition, a telecommunications operator or postal operator must report to the Investigatory Powers Commissioner any relevant error of which it is aware.[27]

8.44. Measures should be implemented to prevent unauthorised disclosure or processing of data. Any suspected or actual unauthorised disclosure or processing of data or information must be reported as set out above.

8.45. Systems must enable the collection of evidence (e.g., audit records) to support investigation into any breach of security.

Additional requirements relating to the destruction of data

8.46. Section 92(2) of the Act makes clear that retained data must be destroyed[28] such that it is impossible to access at the end of the period for which it is required to be retained, unless its retention is otherwise authorised by law. Adequate processes must be put in place to verify that data is deleted and inaccessible at the end of the retention period. Deletions must take place at intervals no greater than monthly. However, telecommunications operators and postal operators should strive to delete data as soon as practically and technically possible at the end of the retention period. If investigators are seeking data that they know may be close to the end of the retention period, Single Points of Contact (SPoCs) should liaise with telecommunications operators and postal operators to see whether any steps can be taken to expedite the request.

8.47. Crypto-shredding (also referred to as Cryptographic Erasure) can be used as an acceptable alternative where data overwriting, or physical destruction of storage media cannot be verified, or is not feasible, such as in cloud environments. Telecommunications operators and postal operators must ensure that:

---

[27] See section 235(6) of the Act. A relevant error is an error by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and of a description identified for this purpose in a relevant code of practice (section 231(9) of the Act). For further details, please also see Chapter 9 of the Interception of Communications Code of Practice.

[28] Section 263(1) of the Act defines 'destroy' in relation to electronic data, for the purposes of the Act, to mean to 'delete the data in such a way as to make access to the data impossible'.

- All encryption keys are generated, stored, and zeroised (deleted) on premises (i.e., outside of the cloud service provider, or any third-party environment).

- All key management practises are documented and auditable if required by the Home Office.

8.48. To prevent future key compromise and/or data reidentification, telecommunications operators and postal operators must ensure strong cryptographic algorithms and modes of operation are used in the generation of all cryptographic keys in compliance with industry standards.

8.49. Telecommunications operators and postal operators must ensure that the cloud service provider can support the data retention, security, and destruction requirements of Communications Data, set out in this code of practice.

8.50. In the case of data not stored in a cloud environment, where the physical, personnel and procedural security measures are assessed by the Home Office (or Information Commissioner) to be sufficient to prevent unauthorised physical access to the data retention system, then data should be deleted in such a way that protects against data recovery using non-invasive attacks (i.e. attempts to retrieve data without additional assistance from physical equipment).

8.51. Where the implemented security measures are assessed by the Home Office (or Information Commissioner) to be insufficient to protect the data retention system against physical access by unauthorised personnel, then additional requirements for the secure destruction of retained data should be agreed with the Home Office and Information Commissioner on a case-by-case basis.

Additional requirements relating to the disposal of data retention systems

8.52. The legal requirement to ensure deleted data is impossible to access must be taken into account when disposing of any system, or component of a system, which reaches the end of its service life.

8.53. If the equipment is to be re-used and it is not stored in a cloud environment, it must be securely sanitised by means of overwriting using a government approved product. In the case of data stored in a cloud environment, it must be destroyed via crypto-shredding as per paragraphs 8.47 – 8.51. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

8.54. If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction.

8.55. Sanitisation or destruction of data must include retained data copied for back-up and recovery, and anything else that stores duplicate data within the

telecommunications operator and postal operator system, unless retention of the data is otherwise authorised by law.

Additional requirements relating to the disposal of interception and equipment interference systems

8.56. A technical capability notice may require that, when disposing of any system, or component of a system, which reaches the end of its service life, an operator must ensure that data is deleted in such a way that it is impossible to access in the future.

8.57. If the equipment is to be re-used, it must be securely sanitised by means of overwriting using a Government-approved product. If the equipment is not to be re-used immediately, it must be securely stored in such a way that it may only be re-used or disposed of appropriately.

8.58. If the equipment is to be finally disposed of, it must be securely sanitised by means of physical destruction by a Government-approved supplier. In the case of interception systems, NTAC can provide further advice to the relevant telecommunications operator or postal operator.

8.59. Sanitisation or destruction of interception identifiers/factors or information used to identify relevant equipment must include retained copies for back-up and recovery, and anything else that stores duplicate data within the operator's system, unless retention of this is otherwise authorised under this Act or another enactment.

Location of retained data

8.60. The location of retained data will be relevant to the security of the data but is only one of a number of factors which are relevant – such as the specific technical security protections. Ensuring the data is retained securely is more important than a general requirement on where the data must be retained that does not take account of specific circumstances.

8.61. The principles of only transferring data when it is consistent with data protection requirements and ensuring the data is retained to an appropriate level of security will apply.

National Security Notices

9. National Security Notices

9.1. The Act provides that the Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of such specified steps as the Secretary of State considers necessary in the interests of national security. A notice can be given only if the Secretary of State is satisfied that the steps required are necessary in the interests of national security and proportionate. Detail on the definition of a telecommunications operator is provided in paragraph 2.1 of this Code.

9.2. Chapter 3 provides information on the type of support that may be required by a national security notice. It also explains where a warrant or authorisation under the Act, the Intelligence Services Act 1994 (ISA), the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) may be required in addition to the notice.

The Activity authorised by a National Security Notice

9.3. Section 252 of the Act states that a Secretary of State may give a notice to a telecommunications operator in the UK requiring the taking of specified steps as the Secretary of State considers necessary in the interests of national security. A notice can only be given if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by the conduct. Subsection (8) makes clear that conduct required by a national security notice is lawful for all purposes.

9.4. The Act does not set out an exhaustive list of the type of conduct that might be required by a national security notice. Section 252(3) does however provide that a notice may, in particular, require an operator:

- to carry out any conduct for the purpose of facilitating anything done by an intelligence service;
- to carry out any conduct for the purpose of dealing with an emergency;
- to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively.

9.5. In practice, the steps that an operator may be required to take include the provision of services or facilities which would help an intelligence service in safeguarding the security of their personnel and operations, or in providing assistance with an emergency as defined in section 1 of the Civil Contingencies Act 2004. An emergency is described in that Act as:

a) an event or situation which threatens serious damage to human welfare in a place in the UK;

b) an event or situation which threatens serious damage to the environment of a place in the UK , or
c) war or terrorism, which threatens serious damage to the security of the UK.

9.6. It is not possible to list the full range of steps that telecommunications operators may be required to take in the interests of national security; not only would this affect the ability of the police and security and intelligence agencies to carry out their work, but as communications technology changes the Secretary of State will need to retain flexibility to respond. However, a notice may typically require a telecommunications operator to provide services to support secure communications by the intelligence services, for example by arranging for a communication to travel via a particular route in order to improve security, or asking a telecommunications operator to refrain from doing something they might otherwise do. A national security notice might relate to the confidential provision of services to the intelligence services by a telecommunications operator, such as by requiring the operator to maintain a pool of trusted staff for the management and maintenance of sensitive communications services.

Limitations as to what can be Authorised by a National Security Notice

9.7. Section 252(4) and (5) restrict when a national security notice can be given. These provisions provide a number of safeguards.

9.8. **A notice cannot be given when the main purpose of the notice is something for which a warrant or authorisation under a relevant enactment is required.** Section 252(6) defines relevant enactments as: the Act, ISA, RIPA, and (RIP(S)A). For example, a national security notice cannot be used as an alternative to an interception warrant where such a warrant is required to authorise the activity. The notice may require the taking of a step that involves conduct that could be authorised under one of the relevant enactments, but that conduct cannot be the main purpose of the notice.

9.9. Secondly, where a notice requires the taking of a step that must be authorised under a relevant enactment, the Act mandates that a warrant or authorisation under one or more of the relevant enactments must be obtained[29]. For example, this might occur where the notice requires an operator to provide a service and one of the steps involved in the provision of that service involves the obtaining of communications data. The obtaining of such data (which cannot be the main purpose of the notice) would need to be authorised under the relevant provisions in the Act. When authorised, the acquisition and use of the communications data would be subject to the usual safeguards that apply to such authorisation regardless of the presence of the notice.

[29] Section 252(4).

9.10. In addition to the limitations detailed above, the Secretary of State must have particular regard to circumstances where a notice requires the taking of any steps that involve an interference with privacy (such as the acquisition of private data) for which a warrant or authorisation under a relevant enactment is not required. In such circumstances, the Secretary of State must be satisfied that a warrant or authorisation is not required, and must, when deciding to give the notice, consider whether it is necessary and proportionate for the data to be acquired. For example, an operator may provide a service to an agency. The agency might require information about staff involved in providing the service for security purposes. This would be an interference with privacy, but it isn't something for which a warrant or authorisation is required.

Necessity and Proportionality

9.11. The Act provides that a national security notice can only be given if the notice is necessary in the interests of national security, and the conduct required is proportionate to what is sought to be achieved by that conduct.

9.12. Any assessment of proportionality involves balancing the reasonableness of the steps that must be taken, against the need for the activity in the interests of national security. The conduct authorised should offer a realistic prospect of bringing the expected benefit and should not be disproportionate or arbitrary.

9.13. Paragraph 2 of Schedule 7 of the Investigatory Powers Act 2016 provides that a code issued under the Act must contain particular provision designed to protect the public interest in the confidentiality of sources of journalistic information and any data which relates to a member of a profession which routinely holds items subject to legal privilege or confidential information. Where a notice requires the taking of a step that involves an interference with privacy, and a warrant or other authorisation has been obtained to authorise that conduct, the Code of Practice relevant to that authorisation will contain provisions required by paragraph 2 of Schedule 7 of the Act. Where a warrant or authorisation is not required to authorise an interference with privacy, it will never be appropriate to obtain journalistic information or any data which relates to a member of a profession which routinely holds material of this nature via a national security notice. As such, it is not necessary to include more detailed safeguards in respect of such information in this code as they are not relevant.

Consultation with Operators

9.14. As set out at paragraph 9.16, before giving a notice, the Secretary of State must consult the operator. In practice, consultation is likely to take place well in advance of a notice being given in order that the operator understands the aims of the notice, can consider the impact of the notice and can work with the

Secretary of State to agree how to deliver the required service. The Secretary of State will also provide advice and guidance to the operator to prepare them for the possibility of receiving a notice. The time taken for the consultation will vary depending on the individual circumstances in each case, such as the complexity of the notice, the nature of the obligations to be imposed, and the resources available to the operator to consider the proposed obligations.

9.15. In the event that the Secretary of State considers it appropriate to give a notice, the Government will take steps to consult the telecommunications operator formally before the notice is given. Should the person to whom the notice is to be given have concerns about the reasonableness, cost or technical feasibility of requirements to be set out in the notice, these should be raised during the consultation process. Any concerns outstanding at the conclusion of these discussions will be presented to the Secretary of State and will form part of the decision-making process.

Matters to be Considered by the Secretary of State

9.16. Section 255(2) provides that before giving a notice to an operator, the Secretary of State must consult the operator. More detail on the consultation is set out in paragraph 9.17 of this Code. Following the conclusion of consultation with a telecommunications operator, the Secretary of State will decide whether to give a notice. This consideration should include all the aspects of the proposed notice. It is an essential means of ensuring that the notice is justified and that proper processes have been followed.

9.17. As part of the decision the Secretary of State must take into account, amongst other factors, the matters specified in section 255(3):

- the likely benefits of the notice;
- the likely number of users of any telecommunications service to which the notice relates, if known;
- the likely cost of complying with the notice – this will include the costs of any requirements or restrictions placed on the telecommunications operator as part of the notice, such as those relating to security, as well as the cost to Government. This will enable the Secretary of State to consider whether the imposition of a notice is affordable for the operator and is both affordable and represents value for money for Government; and
- any other effect of the notice on the telecommunications operator – again taking into account any representations made by the company.

9.18. In addition to the points above, the Secretary of State should consider any other issue which is relevant to the decision. Section 2 of the Act sets out the general

duties that apply to public authorities in relation to privacy. The duties include a requirement on the Secretary of State to have regard to the following when giving, varying, or revoking a notice so far as they are relevant:

- whether what is sought to be achieved by notice could reasonably be achieved by other less intrusive means;
- the public interest in the integrity and security of telecommunication systems; and
- any other aspects of the public interest in the protection of privacy.

9.19. When considering the public interest in the integrity and security of telecommunications systems, the Secretary of State should consider specifically the integrity and security of telecommunications systems impacted by obligations set out in the notice.

9.20. Section 2(3) of the Act acknowledges the need to take other considerations into account, including but not limited to the considerations set out at section 2(4). In cases where a national security notice is to be given, the considerations set out at section 2(4) may not be relevant but where they are relevant, they must be taken into account.

9.21. In addition to the points above, the Secretary of State should consider any other issue which is considered to be relevant to the decision.

Format of National Security Notice Applications

9.22. Responsibility for giving a national security notice rests with the Secretary of State. An application to the Secretary of State for a national security notice to be given to a telecommunications operator should contain the following information:

- the purpose of the notice and what it seeks to achieve;
- why it is not possible to achieve the required outcome by using one of the other powers contained in the Act or any other relevant enactment;
- why the notice is necessary in the interests of national security;
- why the activity required by the notice is necessary and how that activity is proportionate to what it seeks to achieve;
- whether the activity proposed is likely to interfere with privacy and if so, why it is not possible to achieve the required outcome by using less intrusive means;

- an assessment of the reasonableness of the steps the telecommunications operator is required to take, and details of the consultation that has taken place with the telecommunications operator to whom the notice will be given; and

- an assessment of risk to the security and integrity of operator's systems and services.

9.23. Where another warrant or authorisation is required (by virtue of Section 252(4)), the application must provide details of the warrant or authorisation that has been or must be obtained. If a notice requires the taking of any steps that involve an interference with privacy for which a warrant or authorisation under a relevant enactment is not required, the application must:

- Set out the known/expected interference or where there is a potential for interference to occur;

- Explain why this specific interference is necessary and proportionate; and

- Describe any mitigating action which will be taken to keep the interference to a minimum.

Giving a National Security Notice

9.24. Paragraph 9.17 details the matters that must be taken into account before a notice can be given and makes clear that an operator must be consulted prior to a notice being given. Section 252 of the Act provides that the Secretary of State may only give a notice if the Secretary of State considers the following tests are met:

- **The notice is necessary in the interests of national security**;

- **The conduct authorised by the notice is proportionate to what it seeks to achieve**;

- **There are satisfactory safeguards in place** (as described in Chapters 4, 5, 6 and 8 of this Code); and

- **Judicial Commissioner approval has been obtained**. The Secretary of State may not give a notice unless and until the decision to give the notice has been approved by a Judicial Commissioner. Section 254 of the Act sets out that the Judicial Commissioner must review the conclusions that have been reached as to whether the notice is necessary, and whether the conduct that would be authorised is proportionate to what is sought to be achieved.

9.25. The notice must specify the period within which the steps specified in the notice are to be taken. The period of time must be one the Secretary of State considers to be reasonable.

Compliance, Disclosure, and Cost of Data Retention, Technical Capability, and National Security Notices

10. Compliance and Disclosure of Data Retention, Technical Capability, and National Security Notices

Judicial Commissioner Approval

10.1. Before a data retention, technical capability or national security notice can be given, the Secretary of State's decision to give it must be approved by a Judicial Commissioner. In deciding whether to approve the Secretary of State's decision to give a data retention, technical capability or national security notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the notice is necessary and whether the conduct it requires is proportionate to what is sought to be achieved. In reviewing these conclusions, the Judicial Commissioner will apply the same principles as would apply on an application for judicial review. The Judicial Commissioner must review the conclusions with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy). If the Judicial Commissioner refuses to approve the decision to give the notice the Secretary of State may either:

- not give the notice; or,
- refer the matter to the Investigatory Powers Commissioner for a decision (unless they have made the original decision).

10.2. If the Investigator Powers Commissioner refuses the decision to give the notice the Secretary of State must not give the notice. There is no further avenue of appeal available.

10.3. The Act does not mandate how the Judicial Commissioner must show or record their decision. In practice, the Judicial Commissioner's decision will normally be communicated in writing on a formal decision sheet. The Act does not, for example, require the Judicial Commissioner to sign a legal instrument. This means that a Judicial Commissioner can provide oral approval to give a notice. It is important that a written record is taken of any such approvals.

Giving a Data Retention, Technical Capability, or National Security Notice

10.4. Once the Secretary of State has made a decision to give a notice and it has been approved by a Judicial Commissioner, arrangements will be made for it to be given to the telecommunications operator or postal operator. During

consultation, it will be agreed who in the company should receive the notice and how it should be provided (i.e., electronically or in hard copy). If no recipient is agreed, then the notice will be given to a senior executive within the company identified by the Secretary of State or their officials.

10.5. Section 97 and 255(6) provides that a data retention notice and technical capability notice may be given to, and impose obligations on, telecommunications operators and postal operators located outside the UK and may require things to be done outside the UK. Where a notice is to be given to a person outside the UK, the notice may (in addition to electronic or other means of service) be given to the telecommunications operator or postal operator:

- by delivering it to the person's principal office within the UK or, if the person does not have an office in the UK, to any place in the UK where the person carries on business or conducts activities; or
- at an address in the UK specified by the person.

10.6. Where a national security notice is given to a telecommunications operator, that person is under a duty to take all the steps required by the notice. This applies to any company in the UK.

10.7. A data retention notice comes into force from the point it is given to the telecommunications operator or postal operator, unless otherwise specified in the notice. It is the coming into force date of the notice that is relevant for calculating the "relevant period" (two years) for the purposes of when the retention notice will lapse unless it is varied or renewed. If the retention notice is varied or renewed, the relevant period starts from the date the notice would have ceased to have effect if it had not been varied or renewed.

10.8. The "relevant period" for a technical capability or national security notice starts from the date the notice is given to the telecommunications operator unless that notice has been varied or renewed. If the technical capability or national security notice is varied or renewed, the relevant period starts from the date the notice would have ceased to have effect if it had not been varied or renewed.

10.9. As set out in section 253(7), a technical capability notice will specify the period within which the telecommunications operator or postal operator must undertake the steps specified in the notice. It will often be the case that a notice will require the creation of dedicated systems. For data retention notices dedicated systems may need to be constructed by the telecommunications operator or postal operators for the retention of communications data. The time taken to design and construct such systems will be taken into account and, accordingly, different elements of the notice may take effect at different times.

10.10. All notices will also specify the telecommunications services or systems to which the obligations will apply.

10.11. Once a data retention notice has been given to a telecommunications operator or postal operator, a copy of the notice and any other relevant information will be sent by the Secretary of State or their officials to the Information Commissioner, who is responsible for auditing the security, integrity, and destruction of retained data (see Chapter 5 for further details).

Duty to Comply

10.12. A person to whom a technical capability notice relating to targeted equipment interference or bulk CD authorisations, or a national security notice is given is under a duty to comply with the notice. The duty to comply is enforceable Part 9 of the Act against a person in the UK by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 198 or any other appropriate relief[30]

10.13. The duty to comply with a technical capability notice relating to targeted or bulk interception warrants, targeted CD authorisations and a data retention notice under Part 4 of the Act is enforceable against a person in the UK and a person outside the UK by civil proceedings by the Secretary of State[31].

10.14. The duty to comply with a national security notice applies despite any other duty imposed by Part 1, or Chapter 1 of Part 2 of the Communications Act 2003.

Conflicts of Law

10.15. When considering whether it is reasonably practicable for an operator outside the UK to take any steps in a country or territory outside the UK, regard must be given to any requirements or restrictions under the law of that country or that are relevant to the taking of those steps. The Secretary of State must work with telecommunication or postal operators to understand any restrictions imposed on the operator and to find ways for the operator to comply in a manner that avoids such conflicts of law. If an operator has concerns meeting specific obligations set out in a notice due to conflicts of law, these should be raised by the operator during the consultation period. The Secretary of State will then take this into account when giving a notice.

[30] See section 255(10)(a)

[31] See sections 95(5) 255(10)(b)

Disclosure of Data Retention, Technical Capability, National Security, and Notification Notices

10.16. The Secretary of State does not publish or release identities of telecommunications operators and postal operators subject to a notice as to do so may identify operational capabilities or harm the commercial interests of companies that have been given a notice. Should criminals become aware of the capabilities of law enforcement then they may alter their behaviours and switch operator making it more difficult to detect their activities of concern.

10.17. Any person to whom a data retention notice, technical capability notice, national security notice or notification notice is given, or any person employed or engaged for the purposes of that person's business, is under a duty not to disclose the existence or contents of that notice to any person, without the permission of the Secretary of State.

10.18. Section 95(2), 255(8) and 258A(8) of the Act prohibits a telecommunications operator or postal operator, or an employee of or a person working on behalf of the operator disclosing the existence of a data retention, technical capability, national security or a notification notice or the content of such a notice to any person without the permission of the Secretary of State. That duty is enforceable by civil proceedings brought by the Secretary of State.

10.19. Section 95(4), 255(8) and 258A(8) of the Act provides for the person to disclose the existence and contents of a data retention, technical capability, national security or a notification notice with the permission of the Secretary of State. Such circumstances might include disclosure:

- to a person (such as a system operator) who is working with the relevant telecommunications operator or postal operator to give effect to the notice;
- to another telecommunications operator whose services or systems are likely to be impacted by the retention of data or maintenance of the technical capability;
- to relevant oversight bodies (with the exception of the Investigatory Powers Commissioners Office (IPCO), where Secretary of State permission is not required for a telecommunications operator or postal operator to disclose the existence of a notice); to the Investigatory Powers Commissioner or another Judicial Commissioner);
- to regulators in exceptional circumstances where information relating to a retention notice, obligation or capability may be relevant to their enquiries; (with the exception of IPCO, see the point above).
- to a legal adviser in contemplation of legal proceedings, or for the purpose of those proceedings;

- to other telecommunications operators or postal operators subject to a data retention, technical capability or national security notice to facilitate consistent implementation of the obligations; and
- in other circumstances notified to and approved in advance by the Secretary of State.

11. Review of a Data Retention, Technical Capability, or National Security Notice

11.1. The Act includes provisions for telecommunications operator or postal operator to request a review of the requirements imposed on them by a data retention, technical capability, or national security notice, should they wish to do so. A person may refer the whole or any part of a notice back to the Secretary of State for review under sections 90 and 257 of the Act.

11.2. The circumstances and timeframe within which a telecommunications operator or postal operator may request a review and timeframes within which a review must be completed are set out in regulations made by the Secretary of State and approved by Parliament. These circumstances include opportunities for a telecommunications operator or postal operator to refer a notice for review following the receipt of a new notice or the notification of a variation or renewal of a notice. Details of how to submit a notice to the Secretary of State for review will be provided either before or at the time the notice is given.

11.3. During the review period telecommunication operators or postal operators are not required to make changes to specifically comply with the notice which they have referred for review, and operators can continue to make changes to their services and systems. However, they must not make any changes that if implemented would have a negative effect on the capability of the operator to provide any assistance in relation to any warrant, authorisation or notice issued or given under the Act.

11.4. Before deciding the review, the Secretary of State must consult and take account of the views of the Technical Advisory Board (TAB) and a Judicial Commissioner. The TAB must consider the technical requirements and the financial consequences of the notice for the person who has made the referral. The Investigatory Powers Commissioner will consider whether the notice is proportionate.

11.5. The Judicial Commissioner and the TAB must give the relevant telecommunications operator or postal operator and the Secretary of State the opportunity to provide evidence and make representations to them before reaching their conclusions. Both bodies must report these conclusions to the person who made the referral and the Secretary of State.

11.6. The Investigatory Powers (Notification Notices, Review Periods and Technical Advisory Board) Regulations [2025] set out the period of time within which a review must be completed. The review period is defined as the point at which an operator requests the Secretary of State to review a notice, up until the point

the Secretary of State, having received the reports from both the TAB and the Judicial Commissioner, decides whether to revoke, vary or give the notice confirming its effect. The review period can only be extended with the agreement of the Secretary of State, the Judicial Commissioner and the operator. The extension may be for any period mutually agreed, and further extensions can be agreed where necessary. The regulations provide that the review must be completed within 180 calendar days.

11.7. The relevant period is a subsect of the review period and can be defined as the point at which the Secretary of State receives reports from both the TAB and the Judicial Commissioner, up until the point the Secretary of State decides whether to revoke, vary or give the notice.

11.8. The relevant period can be unilaterally extended by the Secretary of State in exceptional circumstances. However, if this extension would exceed the review period then the extension cannot be unilateral and the agreement of the Judicial Commissioner and the operator is required. The regulations provide that the relevant period is 30 calendar days. Exceptional circumstances include but are not limited to:

- Where there is a change of holder of office of the Secretary of State.
- Where there is a terrorist incident or other national security emergency.

11.9. Sections 90(9A) and 257(8A) of the Act include provisions for the Judicial Commissioner to give directions to the operator concerned or the Secretary of State specifying the period within which the operator and Secretary of State may provide evidence or make representations to both the Investigatory Powers Commissioner and the TAB. Section 90(9B) and section 257(8B) also allow the Judicial Commissioner and the TAB to disregard any evidence or representations provided outside those timeframes.

11.10. After considering reports from the TAB and the Investigatory Powers Commissioner, the Secretary of State may decide to vary, revoke, or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision. Until the Secretary of State's decision is approved, there is no requirement for the telecommunications operator or postal operator to comply with the notice so far as referred. Notwithstanding the review, the telecommunications operator or postal operator may be required to provide assistance in giving effect to a warrant or authorisation, and operators cannot make any changes during the review period that will have a negative effect on a capability to provide such assistance.

11.11. Telecommunications operators will not be prevented from carrying out routine security patches during the review period. See section 15.10 for further detail on security patches.

11.12. Where a technical capability notice is subject to a review the duty to comply in section 66 remains in effect in relation to individual authorisations made under Part 3 of the Act.

11.13. Where a data retention notice applies to more than one telecommunications operator or postal operator then only the operators(s) who referred the notice is exempt from the requirement to comply.

11.14. Where a referral is made in respect of a data retention notice the Information Commissioner should be notified by the Secretary of State or their officials.

12. Costs

12.1. Section 249 of the Act recognises that telecommunications operators and postal operators incur expenses in complying with requirements in the Act, including the disclosure of communications data in response to authorisations or notices under Part 3 of the Act, the retention of communications data under Part 4, and notices to maintain technical capabilities or steps required by a national security notice under Part 9. The Act, therefore, allows for appropriate contributions to be made to telecommunication operators and postal operators to cover these costs.

General Considerations on Appropriate Contributions

12.2. Any telecommunications operator or postal operator seeking to recover appropriate contributions towards its costs should make available to the Secretary of State such information as the Secretary of State requires, in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the telecommunications operator or postal operator.

12.3. As costs are reimbursed from public funds, telecommunications operators and postal operators should consider value for money when procuring, operating, and maintaining the infrastructure required to comply with a notice. As changes to the operator's business may necessitate changes to data retention systems, interception systems and equipment interference systems, telecommunications operators and postal operators should take this into account when altering business systems and should notify the Secretary of State of proposed changes.

12.4. Any telecommunications operator or postal operator that has claimed contributions towards costs may be required to undergo a Government audit before contributions are made by the Secretary of State. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

Contributions of Costs for the Acquisition and Disclosure of Communications Data

12.5. The following sections outline the circumstances where the Government will make contributions towards the costs of complying with Parts 3 and 4 of the Act. Telecommunications operators and postal operators who are required to retain communications data will inevitably be required to disclose communications data in response to lawful authorisations or notices. In those circumstances the

Government will make contributions towards the costs of both retaining and disclosing the data. However, most telecommunications operators and postal operators that are required to disclose data are unlikely to be the subject of a data retention notice. In those circumstances they will only be asked to disclose data that they retain for business purposes. For such telecommunications operators and postal operators, the Government will only make contributions towards the costs of disclosing the data in response to authorisations under Part 3 of the Act.

12.6. Significant public funding is made available to telecommunications operators and postal operators to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate, and lawful requirements for the disclosure and acquisition of communications data in support of their investigations and operations to protect the public and to bring to justice those who commit crime.

12.7. An effective and efficient response requires the timely disclosure of communications data. In this code 'timely disclosure' means that ordinarily a telecommunications operator or postal operator should disclose data within agreed service levels or, where there are no agreed service levels[32] within ten working days of being required to do so.

12.8. It is legitimate for a telecommunications operator or postal operator to seek contributions towards its costs which may include funding of those general business overheads required in order to facilitate the timely disclosure of communications data.

12.9. This is especially relevant for telecommunications operators or postal operators which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems or where, in smaller telecommunications operators or postal operators, additional resources may be required to facilitate the response to such authorisations.

12.10. Contributions may also be appropriate towards costs incurred by a telecommunications operator or postal operator which needs to update its systems to maintain, or make more efficient, its disclosure process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the disclosure and acquisition of communications data relating to the use of such services.

[32] Defined service levels may be agreed between the Secretary of State and telecommunications operator or postal operator, for example where a retention notice includes requirements to provide for data to be transmitted efficiently and effectively in response to requests. Such service levels may be specified in the notice.

12.11. Where a telecommunications operator or postal operator identifies that an authorisation or notice for data may result in significant costs it may discuss this with the public authority before complying with the request. This may be a relevant consideration as to whether the authorisation or notice is reasonably practicable.

Contribution to the Costs for the Retention of Communications Data

12.12. The above considerations may be appropriate for all telecommunications operators or postal operators that are required to disclose data. The following considerations only apply to those telecommunications operators or postal operators that are subject to a retention notice under Part 4 of the Act. They are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a data retention notice and the Act.

12.13. Any contribution towards these costs must be agreed by the Home Office before work is commenced by a telecommunications operator or postal operator and will be subject to the Home Office considering, and agreeing, the solution proposed by the telecommunications operator or postal operator.

12.14. These costs may include the procurement or design of systems required to retain communications data, their testing, implementation, continued operation and where appropriate sanitisation and decommissioning. Some overheads may be covered if they directly relate to costs incurred by telecommunications operators or postal operators in complying with their obligations outlined above. Costs may also include costs related to feasibility studies conducted during the period in which a telecommunications operator or postal operator is being consulted prior to a retention notice being given.

12.15. This is especially relevant for telecommunications operators and postal operators that employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke information systems or where, in smaller telecommunications operators or postal operators, additional resources may be required to comply with the requirements in a notice.

12.16. Contributions may also be appropriate towards the costs incurred by a telecommunications operator or postal operator to update its systems to maintain, or make more efficient, its retention process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services.

12.17. A data retention notice must specify the level or levels of contribution to be made in respect of the costs incurred in complying with the notice. Accordingly no changes can be made to the level of contribution without the data retention notice being varied.

Contribution of Costs for the Maintenance of a Technical Capability

12.18. Telecommunications operators and postal operators that are subject to a technical capability notice under Part 9 of the Act are able to recover a contribution towards these costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act.

12.19. Any contribution towards these costs must be agreed by the Secretary of State before work is commenced to develop, install, or operate the capability. Furthermore, the Secretary of State must be satisfied that the proposed capability will meet the requirements set out in the notice.

12.20. Costs that may be recovered could include those related to the procurement or design of systems required to intercept communications, their testing, implementation, continued operation and, where appropriate, sanitisation and decommissioning. Certain overheads may be covered if they relate directly to costs incurred by telecommunications operators or postal operators in complying with their obligations outlined above. This is particularly relevant for telecommunications operators and postal operators that employ staff specifically to manage compliance with the requirements under the Act, supported by bespoke information systems. Further guidance with respect to cost recovery will be made available to all telecommunications operators and postal operators who maintain an interception capability.

12.21. It may also be appropriate for the Government to contribute towards costs incurred by a telecommunications operator or postal operator to update its systems to maintain, or make more efficient, its interception process. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to comply with requirements for the use of such services. However, where a telecommunications operator or postal operator expands or changes its network for commercial reasons, the Government is not required to contribute and the operator is expected to meet any capital costs that arise.

Contribution to the Costs of Taking the Steps Required by a National Security Notice

12.22. To ensure that operators can take the steps set out in a notice, public funding will be made available to contribute towards costs that the operator would not otherwise have incurred when conducting their normal business practices.

12.23. It is legitimate for an operator to seek contributions towards its costs which may include an element of providing funding of those general business overheads required in order to take the steps specified by a national security notice.

12.24. This is especially relevant for operators which employ staff specifically to manage compliance with the requirements made under the Act, supported by bespoke systems.

12.25. Contributions may also be appropriate towards costs incurred by an operator which needs to update its systems to maintain, or make more efficient, the taking of steps required by a national security notice. Similarly, contributions may be appropriate where the provision of new services will require investment in technology in order to take the steps specified in the notice.

12.26. The cost of complying with the requirements in a notice will be discussed during the consultation before a notice is given. Any operator seeking to recover appropriate contributions towards its costs should make available to the Secretary of State such information as the Secretary of State requires in order to provide assurance that proposed cost recovery charges represent an appropriate contribution to the costs incurred by the operator.

12.27. Any operator that has claimed contributions towards costs may be required to undergo a Government audit before payments are made. This is to ensure that expenditure has been incurred for the stated purpose. An audit may include visits to premises, the inspection of equipment, access to relevant personnel, and the examination of documents or records.

12.28. The level of contribution which the Secretary of State determines should be made in respect of the costs incurred, or likely to be incurred, by the telecommunications operator in complying with the notice must be specified on the notice.[33]

Power to Develop Compliance Systems

12.29. In certain circumstances it may be more economical for products to be developed centrally, rather than telecommunications operators, postal operators or public authorities creating multiple different systems to achieve the same

[33] See section 249(7).

end. Where multiple different systems exist, it can lead to increased complexity, delays and higher costs when updating systems (for example, security updates).

12.30. Section 250 of the Act provides a power for the Secretary of State to develop compliance systems. This power could be used, for example, to develop consistent systems for use by telecommunications operators and/or postal operators to intercept communications and obtain secondary data. Such systems could operate in respect of multiple powers under the Act.

12.31. Where such systems are developed for use by telecommunications operators and/or postal operators, the Secretary of State will work closely with such operators to ensure the systems can be properly integrated into their networks.

Regular Review, Variation, Revocation, and Renewal of Data Retention, Technical Capability, and National Security Notices

13. Regular Review, Variation, Revocation, of Data Retention, Technical Capability, and National Security Notices

Regular Review

13.1. Section 90(13) and 256(2) of the Act imposes an obligation on the Secretary of State to keep a notice under regular review. This helps to ensure that the notice itself, and any of the requirements specified in a notice, remains necessary and proportionate.

13.2. This evaluation differs from the process provided for in the rest of section 90 and section 257 of the Act, which permits telecommunications operators and postal operators to refer a notice back to the Secretary of State for a review (see Chapter 11 for further details). It also differs from sections 94A and 256A of the Act, which require a notice to be renewed if it has not been varied, renewed, or revoked in two years.

13.3. It is recognised that, after a notice or variation is given, a telecommunications operator or postal operator may require time to take the steps outlined to put the necessary capabilities in place to meet their obligations. Until these capabilities are fully operational, it will be difficult to assess the benefits of a notice. As such, unless it is necessary to determine that the operator is on course to meet the requirement, the first review should not take place until after the relevant steps have been taken.

13.4. The exact timing and scope of the review is at the Secretary of State's discretion. A review may be initiated for a number of reasons. These include:

- significant change in operational demands by the relevant authorities that calls into question the necessity and proportionality of the notice as a whole, or any element of the notice;
- significant change in the telecommunications operator's or postal operator's activities or services;
- a significant refresh or update of the operator's systems;
- Where a telecommunications or postal operator identifies other changes that could have a bearing on necessity and proportionality; or

- where the notice contains a certain date by which the telecommunications operator or postal operator must comply with the requirement. In such circumstances, an early review might be appropriate to determine the telecommunications operator or postal operator is on course to meet that requirement.

13.5. If a review is required, as with the process for giving a notice, the Secretary of State will consult operational agencies and telecommunications operators or postal operators as part of the review. In addition, the Home Office will consult the Information Commissioner as part of the data retention notice review.

13.6. In relation to data retention notices, the review will also take into account retention period, the number of law enforcement authorisations or notices made, and the age of the data obtained. An absence – or low volume – of law enforcement authorisations or notices will not necessarily mean that it is no longer necessary and proportionate to maintain a data retention notice.

13.7. Once this review process is complete, the Secretary of State will consider whether the notice remains necessary and proportionate. A review may conclude that the notice should continue to remain in force, be varied to add or remove obligations, or be revoked. The relevant telecommunications operator or postal operator, the operational agencies, the Investigatory Powers Commissioner and (in relation to data retention notices) the Information Commissioner will be notified of the outcome of the review.

Variation of Notices

13.8. The communications market is constantly evolving and telecommunications operators or postal operators subject to notices will often launch new services or generate new data that relevant public authorities may require.

13.9. Section 94(4) of the Act provides that a data retention notice may not be varied so as to require the retention of additional relevant communications data, unless the Secretary of State considers the variation to be necessary and proportionate for one or more purposes falling within paragraphs (i) – (vi) of section 87(1)(a) and the decision to vary the notice has been approved by a Judicial Commissioner.

13.10. Section 256(4) of the Act provides that technical capability and national security notices may be varied by the Secretary of State only if the Secretary of State considers that the variation is necessary in the interests of national security and the conduct required by the notice as varied is proportionate to what is sought to be achieved.

13.11. Where the notice as varied imposes further obligations on the operator, the decision to vary a notice must be approved by a Judicial Commissioner. Judicial

Commissioner approval is not required where a variation removes or reduces obligations from the notice.

13.12. Where a telecommunications operator or postal operator has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Secretary of State, in consultation with the telecommunications operator or postal operator, must consider whether the existing notice should be varied.

13.13. Before varying a notice, the Secretary of State must consult the telecommunications operator or postal operator to understand the impact of the change and must consider the same factors as when deciding to give a notice, including cost and technical implications. The Secretary of State or a person acting on their behalf should also consult public authorities to understand the operational impact of any change to the notice.

13.14. Further detail on consultation process and matters to be considered by the Secretary of State can be found in Chapters 4, 7, and 9 of this Code.

13.15. Once a variation has been agreed by the Secretary of State and, where the notice is varied to include the retention of additional data or imposes further obligations, approved by a Judicial Commissioner, arrangements will be made for the telecommunications operator or postal operator to receive notice of this variation and details of the timeframe in which steps specified in the notice as varied should be taken by the telecommunications operator or postal operator. The time taken to implement these changes will be taken into account and, accordingly, different elements of the variation may take effect at different times.

Variation of Data Retention Notices

13.16. Telecommunications operators and postal operators that have been given a data retention notice must notify the Secretary of State of changes to existing telecommunications or postal services covered by the notice and the development of new services and relevant products. Notification should be provided at the earliest practical opportunity and in advance of the service being launched. This includes the TO providing the Home Office with cost estimates and timelines for any projects as soon as reasonably possible. This is important to ensure that obligations under a data retention notice continue to be met. This will enable the Secretary of State to consider whether it is necessary and proportionate to require the telecommunications operator or postal operator to modify an existing capability and/or to require data generated or processed while providing those services to be retained.

13.17. Certain changes to services, such as upgrades of systems or changes to data which are already covered by the existing notice, may be agreed between the Secretary of State and the telecommunications operator or postal operator in question where the change would not require new obligations to be imposed on the company. However, significant changes to networks or service which

necessitate new obligations being imposed on the company will require a variation of the data retention notice. The operator must work with the Secretary of State's representatives to make any technical changes required to ensure that the company can meet the requirements of their notice or the notice as varied.

13.18. There are a number of reasons why a notice might be varied. These include:

- a telecommunications operator or postal operator launching new services or generating new categories of communications data which may be of interest to relevant public authorities;
- Changing law enforcement demands and priorities, including removing a requirement to retain data when no longer necessary and proportionate;
- a recommendation following a review (see paragraph 13.7 above); or
- to amend or enhance the security requirements – for example following an audit of the security, integrity, and destruction of retained data by the Information Commissioner.

13.19. Once a variation notice has been given to a telecommunications operator or postal operator a copy will be sent to the Information Commissioner.

13.20. A data retention notice may be varied to reduce, or extend, the period for which data can be retained. No retention notice, or such variation, can result in data being retained for longer than 12 months.

Variation of Technical Capability Notices

13.21. Telecommunications operators and postal operators that have been given a technical capability notice are required by regulations[34] to notify the Secretary of State of proposed changes to existing telecommunications services and the development of new services and relevant products. Notification should be provided at the earliest practical opportunity and in advance of the service being launched. This will enable the Secretary of State to consider whether it is necessary and proportionate to require the telecommunications operator or postal operator to modify an existing capability or provide a new technical capability on the service.

13.22. The Regulations may include an obligation for an operator that has been given a technical capability notice to provide and maintain arrangements to notify the Secretary of State of proposed changes to telecommunications systems or services. The Secretary of State and a Judicial Commissioner must be content that the level of notification required is necessary and proportionate to what is

[34] The Investigatory Powers (Technical Capability) Regulations 2018 (SI/2018/353) (see paragraphs 13 of Schedules 1 and 2, and paragraph 11 of Schedule 3).

sought to be achieved, and that it is reasonably practicable to impose this requirement on the relevant operator. As detailed at paragraph 7.11, if the operator has any questions or concerns about any of the obligations in the notice, they will have the opportunity to raise these during the consultation process.

13.23. Where a proposed change to an existing telecommunication system or service jeopardises the operator's ability to give effect to an extant notice, the operator must notify the Secretary of State within a reasonable time, as provided for by the Investigatory Powers (Technical Capability) Regulations 2018. NTAC should also be notified of such changes. Certain changes to services, such as upgrades of systems, which are already covered by the existing notice, may be agreed between the Secretary of State and telecommunications operators or postal operators in question, where the change would not require new obligations to be imposed on the company. However, significant changes to networks or service which necessitate new obligations being imposed on the company will require a variation of the technical capability notice. The operator must work with the Secretary of State's representatives and NTAC to make any technical changes required to ensure that the company can meet the requirements of their notice or the notice as varied.

13.24. There are a number of reasons why a notice might be varied. These include:

- a telecommunications operator or postal operator launching new services;
- changing intercepting authority demands and priorities;
- a recommendation following a review (see paragraph 13.7 above); or
- to amend or enhance the security requirements.

Revocation of Data Retention, Technical Capability, and National Security Notices

13.25. Section 94 and 256 provides for the revocation of a data retention, technical capability and national security notice.

13.26. A data retention notice must be revoked (in whole or in part) if it is no longer necessary to require the relevant telecommunications operator or postal operator to retain communications data, or certain types of communications data.

13.27. A technical capability notice must be revoked (in whole or in part) if it is no longer necessary to require a telecommunications operator or postal operator to provide a technical capability or if it is no longer reasonable to impose certain obligations on the operator.

13.28. Circumstances where it may be necessary to revoke a data retention or technical capability notice include where a telecommunications operator or postal operator no longer operates or provides the services to which the notice relates, where operational requirements have changed, or no longer include the data covered by the retention notice, or where such requirements would no longer be necessary or proportionate.

13.29. Circumstances where it may be necessary to revoke a national security notice include where the steps specified in the notice are no longer necessary or proportionate, where an operator no longer operates or provides the services to which the notice relates, or where operational requirements have changed.

13.30. The revocation of a data retention, technical capability or national security notice does not prevent the Secretary of State issuing a new notice, covering the same, or different, data and services to the same telecommunications operator or postal operator in the future, should it be considered necessary and proportionate to do so.

13.31. For data retention notices, once notice of revocation has been given to a telecommunications operator or postal operator, a copy will be sent to the Information Commissioner.

Renewal of Data Retention, Technical Capability, and National Security Notices

13.32. Sections 94A and 256A provides for the renewal of a data retention, technical capability and national security notice by the Secretary of State.

13.33. A renewal of a notice is required if two years has passed since the notice came into force, if it has been varied to include additional obligations or has been renewed. If a notice requires renewal, it must be renewed within the 30-day period ending with the day at the end of which the notice would otherwise cease to have effect. If a notice is not renewed within the period it will cease to have effect.

13.34. A notice may be renewed if the Secretary of State considers the requirements in the notice are still necessary, the conduct required by the notice is still proportionate and the decision to renew the notice has been approved by a Judicial Commissioner. The operator must again be consulted before the renewal notice is given.

13.35. When renewing a notice, the operator may request a review of the requirements imposed on them by a data retention, technical capability or national security notice, should they wish to do so. The notice referral process is covered in subsection 12 of this code.

Notification Notices

14. Notification Notices

14.1. Section 258A(1) of the Act gives the Secretary of State the power to give a notification notice to a telecommunications or postal operator. A notification notice will require the telecommunications operator or postal operator to notify the Secretary of State of any relevant changes specified in the notice that the operator intends to make.

14.2. A notification notice provides the Secretary of State, and by extension law enforcement and intelligence agencies, with time to assess and understand the potential impact of the change. It does not give the Secretary of State any power to intervene in the rollout of the operator's proposed change or require the operator to make any technical changes to maintain capabilities, nor does it require the Secretary of State's consent for the rollout of a change to proceed.

14.3. A telecommunications or postal operator may still be required to disclose data in relation to a warrant or authorisation, in circumstances where they are not subject to an existing notice under the Act. A notification notice may therefore be required to enable the Secretary of State to assess any relevant changes that may impact the telecommunications or postal operator's ability to give effect to warrants and authorisations.

14.4. The Secretary of State may give a notification notice to a relevant operator that discloses, or may be expected to disclose, data of significant operational value. The relevant operator must meet the condition of section 258A(12) in being an operator which provides (or has provided) assistance in relation to any warrant, authorisation or notice issued or given under this Act.

14.5. A change made by a small company (i.e., one providing or intending to provide a telecommunications service to fewer than 10,000 persons) will not be a relevant change for the purposes of section 258A and so will not need be subject to a notification notice. A relevant operator that is already subject to a technical capability notice or national security notice and under an obligation to report changes which may affect their obligations under that notice is unlikely to require a notification notice.

Relevant Change

14.6. A relevant change is a change to a service or system provided or controlled by a telecommunications operator or postal operator that would negatively impact Investigatory Powers Act 2016 capabilities and the operator's ability to provide assistance in relation to any warrant, authorisation or notice issued under the Act. Section 258A(2)(b) provides that the Secretary of State may specify in regulations changes that may be included in a notification notice. As set out at regulation 2(2) of the Investigatory Powers (Notification Notices, Review

Periods and Technical Advisory Board) Regulations [2025], relevant changes may include:

- Changes to data retention periods by the operator. An operator will retain data for as long as business requirement dictates. An operator may change their data retention periods at any point.
- Changes in the operator's ability to lawfully provide communications data.
- Changes in the operator's ability to lawfully provide the content of communications.
- Decommissioning of a service. The decommissioning of a service may also require the Secretary of State to vary a notification notice.

14.7. The Secretary of State may also specify other relevant changes in the notification notice.

14.8. Operators provide unique and individual services and may provide specific technical capabilities that will be known between the operator and Secretary of State. For the protection of these capabilities and to ensure that the operator continues to able to provide assistance in relation to any warrant, authorisation or notice issued under the Act, these will be included in the confidential specification agreed between the operator and Secretary of State.

14.9. The factors which are relevant when considering whether a change is likely to have a negative impact on the operator's technical capabilities, and therefore constitutes a relevant change that needs to be notified to the Secretary of State, include:

- The current or expected number of warrants, authorisations or requests issued to the operator;
- The operational importance of data provided in relation to those warrants, authorisations or requests;
- The types of service the operator provides;
- The customer base of the operator; and
- The market share of the operator.

14.10. Examples of relevant changes are listed below, some of which will only be relevant to certain categories of operators:

- Major network updates.

- Introduction of a new telecommunication system that would impact existing capabilities.
- Introduction of new functionality.
- Changes resulting in an increased or decreased potential for collateral intrusion.
- Change in ownership of the relevant operator.
- Change in network architecture, such as, off-shoring services/network components.
- Change in operating methods and procedures for tasking and support.
- Change in the telecommunications operator's ability to meet Service Level agreements or response times.
- Modifications to availability or quality of intercept related information.

14.11. Further information regarding what may constitute a relevant change has been provided in the examples below.

Example 1

A telecommunications operator reduces their data retention period from 6 months to 5 months for data relating to a specific service specified within the operator's notification notice.

Example 2

A telecommunications operator reduces their data retention period from 6 months to 7 days for data relating to a specific service specified within the operator's notice.

Both example 1 and 2 are relevant changes relating to changes to data retention periods by the telecommunications operator and would require the operator to notify the Secretary of State within a reasonable time. Example 2 is a significant reduction in the data retention period, and it is therefore reasonable to expect the Secretary of State to receive more advanced notification for example 2 due to the potential impact of the change. See paragraph 14.20 for more information on "reasonable time".

Example 3

A telecommunication operator is decommissioning a service specified within the operator's notification notice.

This is a relevant change relating to the decommissioning of a service by the telecommunications operator and would require the operator to notify the Secretary of State within a reasonable time. Notification of the decommissioning of a service will allow time for the government to continue to ensure public safety whilst not interrupting the commercial decisions of the company. For example, further warrants may be executed, where necessary and proportionate, within the timeframe notified before the service is decommissioned.

Example 4

A telecommunications operator who has been given a notification notice is being acquired by another company, impacting capabilities relating to services specified within the operator's notification notice.

This is a relevant change relating to one or more of the changes listed in paragraph 14.6 and would require the telecommunications operator to notify the Secretary of State within a reasonable time. As acquisitions can be commercially sensitive, the expectation is that the Secretary of State will be notified as soon as reasonably practicable.

Example 5

A telecommunications operator is making a major update to their network which relates to a system specified within the operator's notification notice.

This is a relevant change relating to one or more of the changes listed in paragraph 14.6 and would require the telecommunication operator to notify the Secretary of State within a reasonable time. This is a large-scale change to a network and the potential to impact lawful access is significant. The Secretary of State requires early notification to ensure the maximum possible time is available to conduct an impact assessment.

Security Patches

14.12. Security patches will not be included within the notification requirement as a relevant change. As defined by the National Cyber Security Centre, a security patch fixes a defect in installed software and leaves the intended functionality of the software unchanged.[35] Any security patch, update or fix that meets this

[35] Keeping devices and software up to date - NCSC.GOV.UK; https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date

definition will not need to be notified. A decision taken by a telecommunications operator to implement additional encryption on any aspect of its services would not fall under this definition, and accordingly might constitute a relevant change.

Consultation with Operators

14.13. Before giving a notification notice, the Secretary of State must consult the telecommunications or postal operator. The consultation will result in an individualised and confidential specification. This will be provided as an annex to the notice and will set out the services and / or systems, specific to the operator, to which the notification requirement applies. The operator will only be required to provide the Secretary of State with a notification of change in relation to these specific services and systems, where the proposed change will result in a negative impact on Investigatory Powers Act 2016 capabilities. Should the operator have any concerns regarding the obligations set out in the notice, this should be raised during the consultation process to ensure the specification accurately reflects the services and systems provided.

Matters to be considered by the Secretary of State

14.14. Following the conclusion of the consultation with the telecommunications or postal operator, the Secretary of State will consider whether to give a notification notice. The Secretary of State may only give an operator a notification notice if they consider it is necessary for maintaining IPA capabilities to ensure the operator can provide assistance in relation to any warrant, authorisation or notice under the Act, and the conduct required by the notice is proportionate.

14.15. Before giving a notice under this section, the Secretary of State must among other matters take into account:

- the likely benefits of the notice, including projected as well as existing benefits;
- the likely number of users (if known) of any postal or telecommunications service to which the notice relates;
- the likely cost of complying with the notice; and
- any other effect of the notice on the operator, taking into account any representations made by the operator.

Conflicts of Law

14.16. When considering whether it is reasonably practicable for an operator outside the UK to take any steps in a country or territory outside the UK, regard must be given to any requirements or restrictions under the law of that country or that are relevant to the taking of those steps and the extent to which it is reasonable practicable to give effect to the warrant in a way that does not breach any of those requirements or restrictions. The Secretary of State must work with telecommunication or postal operators to understand any restrictions imposed on the operator and to find ways for the operator to comply in a manner that avoids such conflicts of law. If an operator has concerns meeting specific obligations set out in a notice due to conflicts of law, these should be raised by the operator during the consultation period. The Secretary of State will then take this into account when giving a notice.

Giving a Notification Notice

14.17. Once the Secretary of State has decided to issue a notification notice, arrangements will be made for it to be given to the telecommunications or postal operator. During the consultation, it will be agreed who in the company should receive the notice and how it should be provided (i.e., electronically or as a hard copy). If no recipient is agreed, then the notice will be given to a senior executive within the company identified by the Secretary of State or their officials.

14.18. A notification notice comes into force from the point it is given to the telecommunications or postal operator, unless otherwise specified in the notice.

14.19. A relevant operator to whom a notification notice is given is under a duty to comply with the notice. The duty to comply with a notification notice is enforceable by civil proceedings by the Secretary of State.

Reasonable Time

14.20. If an operator under a notification notice identifies a relevant change to a service or system set out within that notice, they are required to notify the Secretary of State within a reasonable time before making the relevant change to which the notice applies. As early an indication as possible of a change will allow time for the impact of the change to be assessed and will support efforts for potential mitigations to be fully explored with support from law enforcement and intelligence agencies. For significant changes it is important the Secretary of State has the maximum time available to carry out this assessment. Expectations regarding what is a reasonable time may be agreed between the Secretary of State and the operator during the consultation before the notice is given. It would be impractical to define reasonable time any further, given that

reasonableness will be impacted by factors such as the scale and timing of the proposed change (see also Examples 2, 4 and 5 at paragraph 15.11 above).

Notification Process

14.21. The Secretary of State will confirm receipt of the notice of a relevant change and, with support from law enforcement and intelligence agencies, will conduct an assessment of the impact of the change on Investigatory Powers Act 2016 capabilities. It will allow a formal opportunity for the operator and government to work together and find a solution that will ensure public safety is protected. The Secretary of State will contact the operator within 10 working days of receiving the notification if more information is required.

14.22. The notification of a proposed change will allow law enforcement and intelligence agencies time to assess the impact and adjust working practices where necessary. Should the Secretary of State wish to intervene in any way with the change the operator intends to make, the Secretary of State will use the notices regimes in the same way that is currently available to them. Such a step would only be taken if necessary and proportionate in order to protect Investigatory Powers Act 2016 capabilities.

14.23. If the Secretary of State does consider giving a data retention, technical capability, or national security notice to the relevant operator, the Secretary of State is required to follow the process laid out in the Act and this code for giving such a notice, including the duty to consult the operator. If a data retention, technical capability, or national security notice is subsequently given the decision must be approved by a Judicial Commissioner.

Variation of Notification Notices

14.24. A notification notice may be varied by the Secretary of State if the Secretary of State considers the variation is necessary for maintaining the capability of an operator to provide assistance in relation to any warrant, authorisation or notice issued, and the conduct required is proportionate to what is sought to be achieved.

14.25. For instance, a notification notice may be varied if the operator introduces a new service or system that is not covered by the current notice and the Secretary of State considers that the service or system is of significant operational value to law enforcement and intelligence agencies.

14.26. Where a telecommunications operator or postal operator has changed name, for example as part of a rebranding exercise or due to a change of ownership, the Secretary of State, in consultation with the telecommunications operator or postal operator, must consider whether the existing notice should be varied.

14.27. Before varying a notice, the Secretary of State must consult the telecommunications operator or postal operator to understand the impact of the change and must take into account the same factors as when deciding to give a notice, including likely benefits and cost implications.

14.28. Once a variation has been agreed by the Secretary of State, arrangements will be made for the telecommunications operator or postal operator to be formally notified of this variation.

Revocation of Notification Notices

14.29. A notification notice must be revoked (in whole or in part) if it is no longer necessary or proportionate for the telecommunications or postal operator to be subject to the obligation to notify the Secretary of State of a relevant change to an applicable service or system.

14.30. The revocation of a notification notice does not prevent the Secretary of State issuing a new notice, covering the same, or different, services or systems to the same telecommunications operator or postal operator in the future should it be considered necessary and proportionate to do so.

Oversight of the Notices Regime

15. Oversight

15.1. The Investigatory Powers Act provides for an Investigatory Powers Commissioner, whose remit is to provide comprehensive oversight of the use of all the powers referred to within section 229 of the Act. This includes Technical Capability, Data Retention, and National Security Notices. The Commissioner will be, or will have been, a member of the senior judiciary and will be entirely independent of His Majesty's Government or any of the public authorities authorised to use investigatory powers. The Commissioner will be supported by inspectors and others, such as technical experts and legal experts, qualified to assist the Commissioner in his or her work. The Commissioner will also be advised by the Technical Advisory Panel.

15.2. The Investigatory Powers Commissioner, and those that work under the authority of the Commissioner, will ensure compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Investigatory Powers Commissioner may undertake these inspections, as far as they relate to the Investigatory Powers Commissioner's functions, entirely on his or her own initiative. Section 236 provides for the Intelligence and Security Committee of Parliament to refer a matter to the Investigatory Powers Commissioner with a view to carrying out an investigation, inspection, or audit.

15.3. The Investigatory Powers Commissioner will have unfettered access to all locations, documentation, and information systems as necessary to carry out their full functions and duties. In undertaking such inspections, the Investigatory Powers Commissioner must not act in a way which is contrary to the public interest, or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK (see section 229(6)). A Judicial Commissioner must, in particular, not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, or unduly impede the operational effectiveness of an intelligence service, a police force, a government department or His Majesty's forces (see section 229(7)).

15.4. All relevant persons using investigatory powers must provide all such documents and information, and such assistance as is required, to the Investigatory Powers Commissioner and anyone acting on their behalf, for the purposes of the Commissioner's functions. Here, a relevant person includes, among others, any person who holds, or has held, an office, rank or position with a public authority (see section 235(7)).

15.5. The Investigatory Powers Commissioner must report annually on the findings of their audits, inspections, and investigations. This report will be laid before Parliament and will be made available to the public, subject to any necessary redactions made in the public interest. Such redactions to the Investigatory Powers Commissioner's report may be made by the Prime Minister, after consultation with the Investigatory Powers Commissioner and (where relevant to the functions under Part 3 of the Police Act 1997) the Scottish Ministers. If the Investigatory Powers Commissioner disagrees with the proposed redactions to their report, then the Investigatory Powers Commissioner may inform the Intelligence and Security Committee of Parliament that they disagree with them.

15.6. The Investigatory Powers Commissioner may also report to the Prime Minister, at any time, on any of his or her investigations and findings as they see fit. These reports will also be made publicly available subject to public interest considerations. Public authorities, telecommunications operators, and postal operators may seek general advice from the Investigatory Powers Commissioner on any issue which falls within the Investigatory Powers Commissioner's statutory remit. The Investigatory Powers Commissioner may also produce guidance for public authorities on how to apply and use investigatory powers. Wherever possible this guidance will be published in the interests of public transparency.

15.7. Further information about the Investigatory Powers Commissioner, their office and their work may be found at: www.ipco.org.uk.

The Information Commissioner

15.8. The Act requires that the Information Commissioner provides independent oversight of the integrity, security or destruction of data retained by virtue of Part 4 of the Act. Data is retained by virtue of Part 4 where the retention of that data is specifically required by a retention notice. There will be circumstances where the data might be stored in different systems across an operator's network, for example for business purposes as well as in a dedicated retention store. In such circumstances, the Information Commissioner must audit any system that the telecommunications operator or postal operator uses to comply with the retention requirements in a data retention notice.

15.9. Where data is retained as a consequence of a data retention notice but the telecommunications operator or postal operator has a lawful reason to move or copy the data to a separate store, data retained in the separate store, insofar as it is no longer being retained in order to comply with a retention notice, is not subject to audit by the Information Commissioner under the Act. These circumstances may include where a copy of retained data that has been disclosed under Part 3 of the Act is being kept in the event of later challenge in legal proceedings. Such data must still be kept securely and will be subject to

relevant data protection legislation. However, it is not subject to audit by the Information Commissioner under the Act because the lawful basis for retaining the data will no longer be a retention notice.

15.10. Where data retained under a retention notice is moved to another store and kept for a separate lawful purpose, details of the lawful basis for moving the data and keeping it in a separate store, along with details of the process used, must be kept by the telecommunications operator or postal operator and provided to the Information Commissioner on request. This is to ensure that the Information Commissioner can determine that any processes for accessing retained data comply with the security requirements.

15.11. This code does not cover the exercise of the Information Commissioner's functions. It is the duty of any telecommunications operator or postal operator subject to a notice under the Act to comply with any requests made by the Information Commissioner, in order to provide any information required by the Information Commissioner to discharge their functions. The Information Commissioner may, for example, make requests:

- to access any relevant premises;
- for copies of relevant documentation;
- to inspect any relevant equipment or other material; or
- to observe the processing of relevant communications data.

15.12. Without prejudice to the independence of the Information Commissioner, a telecommunications operator or postal operator may discuss a request from the Information Commissioner and its potential implications with the Home Office.

15.13. Reports made by the Information Commissioner concerning the inspection of telecommunications operators and postal operators and the security, integrity and destruction of communications data retained under the Act may be made available by the Information Commissioner to the Home Office. This can help to promulgate good practice and identify security enhancements and training requirements within telecommunications operators and postal operators. The Home Office will work with telecommunications operators and postal operators to address any recommendations made by the Information Commissioner.

15.14. Subject to discussion between the Information Commissioner and the Home Office, either may publish the inspection reports, in full or in summary, or a single overarching report to demonstrate both the oversight of the security, integrity and destruction of data and telecommunications operators' and postal operators' compliance with the Act. Because of the sensitivity of identifying which companies have received retention notices, any such report must be sufficiently redacted to protect the identities of the companies.

15.15. Section 95(3) of the Act prohibits the Information Commissioner or a member of their staff disclosing the existence of a retention notice or the content of the retention notice to any person without the permission of the Secretary of State.

16. Complaints

16.1. The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of certain investigatory powers, including those covered by this code, as well as conduct by or on behalf of any of the intelligence services and is the only appropriate tribunal for human rights claims against the intelligence services. Any complaints about the use of powers as described in this code should be directed to the IPT.

16.2. The IPT is entirely independent from His Majesty's Government and the public authorities who use investigatory powers. It is made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint or claim from a person, the IPT can undertake its own enquiries and investigations and can demand access to all information necessary to establish the facts of a claim and to reach a determination. A 'person' for these purposes includes any organisation and any association or combination of persons (see section 81(1) of RIPA), as well as an individual.

16.3. This code does not cover the exercise of the Tribunal's functions. Should you wish to find out more information about the IPT or make a complaint, then full details of how to do so are available on the IPT website: www.ipt-uk.com. Alternatively, information on how to make a complaint can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

16.4. If you have received a determination or decision from the IPT that you are not satisfied with then, in certain circumstances, you may have a right of appeal. The IPT will inform you when you have that right of appeal and which court you should apply to in order for your appeal application to be considered.

[leave blank – inside back cover]

XXX-X-XXXX-XXXX-X

XXXXXXXXXXXXX