Home Office

Investigatory Powers Act 2016

Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data

November 2017

Ministerial Foreword

Communications data is the ‘who’, ‘where’, ‘when’, ‘how’ and ‘with whom’ of a communication, but not what was written or said, and includes information such as the subscriber to a telephone service.

The Investigatory Powers Act 2016 provides that communications service providers may be required by the Secretary of State to retain communications data, for up to 12 months, where it is considered necessary and proportionate to do so and where that decision has been approved by a Judicial Commissioner. Specified public authorities, including the police and the security and intelligence agencies, may acquire communications data from a telecommunications operator or postal operator where it is both necessary and proportionate to do so, for specified purposes.

The retention of, and ability to access, communications data is an essential tool for law enforcement and national security investigations. It is used to investigate crime, keep children safe, support or disprove alibis and link a suspect to a particular crime scene, amongst many other purposes. Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud.

On 21 December 2016 the Court of Justice of the European Union (CJEU) handed down its judgment in two cases, including a reference from the Court of Appeal relating to a challenge to the UK’s then legislation governing data retention. The CJEU’s judgment set out requirements that need to be in place for a data retention regime to be considered compliant with EU law.

Part 4 of the Investigatory Powers Act 2016 has since replaced the Data Retention and Investigatory Powers Act 2014, and provisions in Part 3 of that Act will in time replace the provisions in the Regulation of Investigatory Powers Act 2000 which regulate the lawful acquisition of that data by public authorities.

The Government has given careful consideration to the CJEU’s judgment, bearing in mind the importance of communications data as an investigative tool used by those responsible for keeping citizens safe. For example, communications data is often essential to identify paedophiles involved in online child abuse, and can identify where and when these horrendous crimes have taken place.

The Government considers that some aspects of our current regime for the retention of and access to communications data do not satisfy the requirements of the CJEU’s judgment and, therefore, proposes to amend the Investigatory Powers Act 2016.

It is important that any changes support the important right to individual privacy and the collective right of citizens to be protected from crime and terrorism. We must ensure that the police and other specified public authorities can continue to be able to access and use retained communications data in a way that is consistent with requirements of EU law and with our responsibilities to protect the public.

These are issues of public importance, and accordingly the Government is consulting on what changes should be made in response to the judgment. In particular, the consultation sets out what changes we currently propose to make in response to the judgment and,

where no changes are proposed, explains why the Government considers that the regime already addresses the requirements of the CJEU's judgment. We are particularly seeking views on those proposals, although we will consider other changes that consultees suggest should be made as a result of the judgment more generally (save in respect of national security, which we consider to fall outside the scope of EU law, and which is currently the subject of separate legal proceedings).

All responses will be welcomed and carefully considered.

Rt Hon Ben Wallace MP

Minister of State for Security

Contents

Background and overview

Scope of the consultation

Topic of this consultation:	This consultation is on the Government's proposed response to the European Court of Justice (CJEU) ruling relating to the retention and acquisition of communications data.
Scope of this consultation:	This consultation seeks representations on the amendments being proposed to the Investigatory Powers Act 2016 in response to the CJEU ruling and on the accompanying code of practice.
Geographical scope:	UK wide

Basic information

To:	Representations are welcomed from telecommunications operators and postal operators, public authorities that have powers under the Investigatory Powers Act 2016, as well as professional bodies, interest groups and the wider public.
Duration:	7 weeks, closing at 23.59 on 18 January 2018 (6 weeks and an additional week to take account of Christmas)
Enquiries and responses:	*investigatorypowers@homeoffice.gsi.gov.uk* Please indicate in your response whether you are content for it to be published, with or without attributing it to you/your organisation.
After the consultation:	Following the consultation period, responses will be analysed and the draft legislation and draft code revised as necessary. They will then be laid before Parliament for approval.

Background

It is important to put into context the significance of communications data in the prevention and detection of crime: it is used in 95% of serious and organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division, and has been used in every major Security Service counter-terrorism investigation over the last decade.

Figures published annually by the Interception of Communications Commissioner, who was responsible for overseeing public authorities' use of these powers before the function was taken on by the Investigatory Powers Commissioner in September 2017, provide an insight into the level of use by public authorities of this vital tool. They provide details of the number of authorisations given to acquire different types of communications data by the different authorities empowered to do so, and the purposes for which they obtain the data.

From January to December 2015, 761702 items of data were acquired by public authorities, 85.8% of which was for the statutory purpose of preventing or detecting crime or of preventing disorder. And 53% of the data acquired for that purpose was in relation to four crime types: drugs offences, sexual offences, theft offences, and fraud and deception offences.

Following an earlier ruling by the Court of Justice of the European Union (CJEU) in 2014 (Joined Cases C-293/12 and 594/12: *Digital Rights Ireland ltd and Seitlinger*, quashing the EU Data Retention Directive), the UK Parliament legislated for a domestic communications data retention regime through the Data Retention and Investigatory Powers Act 2014 (DRIPA). DRIPA provided for the Secretary of State to, amongst other things, require telecommunications operators and postal operators to retain communications data for a maximum of 12 months, where necessary and proportionate to do so for a number of statutory purposes. DRIPA contained a sunset clause, which meant that the legislation would fall away on 31 December 2016.

The Investigatory Powers Act 2016 (IPA) received Royal Assent on 29 November 2016. Part 4 of the IPA, which replaces the communications data retention provisions in DRIPA, came into force in December 2016. Part 3 of the IPA, which provides for the acquisition of communications data (including retained data) by public authorities, and will replace the relevant provisions in the Regulation of Investigatory Powers Act 2000 (RIPA), has not yet been commenced.

Legal proceedings were brought in 2014 alleging, amongst other things, that DRIPA was incompatible with EU law. Although the Divisional Court ruled against the Government, the Court of Appeal provisionally found broadly in favour of the Government, but referred the case to the CJEU to clarify EU law. The CJEU handed down its judgment on 21 December 2016 (Joined Cases C-203/15 and C-698/15), specifying a number of requirements that need to be in place for a data retention regime to be compliant with EU law, but making it clear that it was a matter for the domestic courts to consider how this judgment should be applied to national legislation.

Following the CJEU ruling, the Government accepted in the domestic litigation that DRIPA, and consequently some aspects of Part 4 of the IPA, are inconsistent with EU law, in that:

a) there is no provision for independent authorisation of requests for access to retained data; and

b) the crime purpose for retaining and accessing data is not limited to serious crime.

In the light of that, Parliament should have the chance to consider what changes to the law should be made in response to the CJEU's judgment. That is particularly so in this case, because the CJEU's judgment leaves considerable discretion to Member States to determine the precise design of their data retention arrangements and this is an area of the law that requires the rights of individual privacy and the safety and security of citizens to be appropriately protected. Parliament will need to consider carefully how these rights should be protected.

In considering our proposed response to the judgment, we have already consulted extensively with the law enforcement and intelligence community, the Investigatory Powers Commissioner and his staff, along with staff in the Office of the Interception of Communications Commissioner, who until recently had oversight of the use of this legislation. We have also engaged with telecommunications operators and postal operators likely to be affected by the legislation.

Why we are consulting

The Government proposes amending the IPA by regulations made under section 2(2) of the European Communities Act 1972. Although the Government does not normally consult on such regulations, given the ongoing public interest in investigatory powers the Government considers it important to consult on potential changes to the legislative regime in order to inform the legislative response and subsequent Parliamentary debate.

Additionally, under the IPA, the Secretary of State is required to issue codes of practice about the exercise of functions under the Act. Schedule 7 to the Act sets out further requirements which the codes must satisfy. Prior to issuing the codes, the Secretary of State must prepare and publish draft codes. This consultation is intended to fulfil those requirements in respect of the communications data code of practice.

Documents forming part of this consultation

As part of this consultation the Government welcomes comments on the amendments that it is proposing to the IPA and on the draft code of practice. Consultation responses are particularly welcomed on the proposed amendments, although the Government will also consider other amendments that consultees consider should be made to the IPA and draft code of practice more generally in response to the judgment. It should also be noted that aspects of Part 4 of the IPA, which are covered by this consultation, are the subject of ongoing litigation, which may have an impact on this consultation and any proposed amendments to the IPA. The next section of this consultation document sets out the Government's position on the scope of the judgment and how the changes being proposed to the legislation and code of practice seek to ensure that the regime meets the requirements of EU law.

The Government is clear, however, that national security activities fall outside the scope of EU law and are not subject to the requirements of the CJEU's judgment, as reflected by article 4(2) of the Treaty of the European Union; *"the Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State"*. This issue is subject to ongoing litigation and a reference is being made to the CJEU on this

point in associated litigation in the Investigatory Powers Tribunal. We are not therefore seeking views on this issue in this consultation.

The draft Data Retention and Acquisition Regulations

The Government proposes to make changes to the IPA through regulations made under section 2(2) of the European Communities Act 1972, which permits the Secretary of State to amend primary legislation by regulations to implement EU law obligations as in this case.

The proposed regulations will be subject to the affirmative procedure, which requires the formal approval of both Houses of Parliament, including a debate and vote in each House, before it becomes law. This consultation will be brought to the attention of relevant Parliamentary committees.

To assist consultees in consideration of the draft Regulations, we have also published a document showing how the relevant parts of the IPA would look if the proposed draft Regulations were approved.

The draft Communications Data Code of Practice

The code of practice sets out the processes and safeguards governing the retention of communications data by telecommunications operators and its acquisition by public authorities, including the police and the security and intelligence agencies. It gives detail on how these powers should be used, including examples where relevant, and is intended to provide additional clarity and ensure the highest standards of professionalism and compliance with these important powers.

The code is primarily intended to guide those public authorities able to exercise powers under the IPA and telecommunications operators and postal operators who may be given data retention notices under the Act.

Once issued, the code of practice will have statutory force, and individuals exercising functions to which the code relates must have regard to it. The code is admissible as evidence in criminal and civil proceedings, and may be taken into account by any court, tribunal or supervisory authority when determining a question arising in connection with those functions.

This draft code of practice takes into account the amendments we propose making to the IPA by way of the draft Data Retention and Acquisition Regulations.

We are consulting on the code of practice at the same time as the draft Regulations, as this allows us to provide more detail on how the new regime will work in practice, when the two documents are read together.

The code was published in draft during the passage of the Investigatory Powers Bill to assist Parliament's consideration of the provisions. In addition to the changes made to the code to reflect the changes we are proposing to the regime, the code has also been updated to provide additional guidance on definitions of a telecommunications operator and provide additional guidance on internet communications data.

Next steps

Following the consultation, the Secretary of State will carefully consider any representations made about the proposed response to the judgment, and what, if any, changes may be required to the draft Regulations and code of practice. The draft Regulations and code of practice will then be laid in Parliament for approval by both Houses before they can come into effect.

Response to the judgment

Summary and scope of the judgment

The CJEU ruled in Joined Cases C-203/15 and C-698/15 that EU law does not permit national legislation that allows for the general and indiscriminate retention of communications data for the purpose of fighting crime. Rather, Member States can legislate for a regime which permits the targeted retention of communications data for the purpose of fighting serious crime, and the judgment sets out conditions that such legislation must satisfy in order to meet these requirements.

The judgment also requires a number of safeguards to be in place before retained communications data can be acquired, including a requirement for prior judicial or independent administrative approval of requests for access to such data.

The remaining parts of this consultation document set out the key safeguards identified in the CJEU's judgment, along with the Government's proposed responses to them.

Application of the judgment to entity data

The IPA updated the definitions of communications data to reflect changes to the way in which communications services operate. The definition of communications data in the IPA creates two distinct categories of data: entity data and events data. The definition of entity data covers information which would previously have been classed under RIPA as subscriber data, while the definition of events data covers information previously classed under RIPA as traffic and service use data. The definitions are contained in section 261 of the IPA, and state as follows:

> *"'Entity data' means any data which-*
>
> *(a) Is about-*
>
> *i. An entity,*
>
> *ii. An association between a telecommunications service and an entity, or*
>
> *iii. An association between any part of a telecommunication system and an entity,*
>
> *(b) Consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and*
>
> *(c) Is not events data.*
>
> *'Events data' means any data which identifies or describes an event (whether or not by reference to its location) on, in, or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at a specific time."*

The CJEU judgment refers to only certain types of communications data - traffic data and location data, as defined in Directive 2002/58/EC ("the ePrivacy Directive"). The definitions of "traffic data" and "location data" in the ePrivacy Directive are as follows:

> *"'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.*

'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.""

The Government's view is that data covered by the definition of "events data" in section 261 of the IPA includes the data covered by the definitions of "traffic data" and "location data" in the ePrivacy Directive. Accordingly, the CJEU's judgment should be read as applying to "events data" but does not apply to the retention or acquisition of "entity data" within the meaning of section 261. Views are sought on the scope of the data covered by the judgment, including how the scope of such data interrelates with the definitions of "events data" and "entity data" in the IPA.

In any event, a number of the changes to the regime will be applied to all communications data applications for the purposes of creating a simpler, more practical regime. Where this is the case, it is set out in further detail below.

Application of the judgment to national security

The EU, and therefore the CJEU, may only act within the limits of the competences conferred upon the EU by the Member States in the EU Treaties. Competences not conferred upon the EU remain with the Member States. Matters of Member States' national security are explicitly identified as being the sole responsibility of Member States in Article 4(2) of the Treaty of the European Union (TEU). The Charter of Fundamental Rights, on which the CJEU's judgment relies in part, only applies to Member States' actions when they are acting within the scope of EU law.

The requirements set out in the judgment were considered by the CJEU to be appropriate where there was a requirement on service providers to retain and disclose communications data for the purposes of the targeted investigation, detection and prosecution of serious crime. The judgment must be read consistently within the context of the jurisdiction conferred on the EU, and therefore on the CJEU, by the Treaties.

Accordingly, the Government's position is that the judgment does not apply to the retention or acquisition of data for national security purposes. The three UK intelligence agencies (MI5, MI6 and GCHQ) primarily exist to manage national security threats to the UK. The Government considers that their activities, including requests for communications data for the statutory purpose of crime, fall outside the scope of EU law and the CJEU's judgment.

The issue of whether the CJEU's judgment applies to the activities of the security and intelligence agencies in relation to the acquisition and use of bulk communications data for the purposes of national security is the subject of a pending reference to the CJEU in proceedings before the Investigatory Powers Tribunal (*Privacy International and (1) SSFCO (2) SSHD (3) GCHQ (4) Security Service (5) Secret Intelligence Service* IPT/15/110/CH). In the circumstances, the Government is not consulting on this issue.

Notwithstanding that position, and without prejudice to the outcome of that litigation, for practical reasons only a number of the proposed changes to the regime will apply to certain national security applications for communications data. This is being proposed in the interests of creating a simpler, more practical regime. Where this is the case, it is set out in further detail below.

Application of the judgment to business data

The judgment, and therefore any obligations and requirements contained within it, relate to communications data that is retained by commercial entities by virtue of an obligation imposed by the Government. Telecommunications operators and postal operators will retain a wide range of communications data in any event for their own business purposes. The Government's view is that none of the requirements of the CJEU's judgment relate to the acquisition of data that is being held for business purposes, rather than pursuant to a retention obligation imposed by Government. Nevertheless, in order to avoid additional complexity for public authorities and for telecommunications operators and postal operators, the Government does not, at present, propose creating separate arrangements governing access to this business data.

Specific requirements of the judgment

Scope and permissibility of the regime

Permissibility of a retention regime

> *"[EU law] must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication." [para. 112 (of the judgment)] "Such limits may be set using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission on such offences." [para. 111] The retention of data must … continue to meet objective criteria that establish a connection between the data to be retained and the objective pursued [para. 110]*

The IPA provides that the Secretary of State can only require a telecommunications operator or postal operator to retain communications data for up to 12 months if it is necessary and proportionate for one or more specified statutory purposes, and the decision to give a notice has been approved by a Judicial Commissioner. A retention notice may relate to more than one telecommunications operator or postal operator, require retention of all or some data generated or processed by the operator, specify different retention periods for different data, and can contain other restrictions or requirements. These other requirements and restrictions can include restrictions on the geographical areas covered by a retention notice, or can exclude certain customers of groups of customers.

Furthermore, section 88 of the Act requires that the Secretary of State's consideration also takes into account, amongst other matters, the likely benefits of the notice, the number of users affected by the notice, the technical feasibility of the requirements it imposes and the likely costs of complying with the requirements of the notice, and any other effect of the notice on the operator.

As with the use of any investigatory power provided for in the IPA, the Secretary of State must consider whether the objective could be achieved by any less intrusive means. Issues such as whether the level of protection to be applied to the data should be higher because of its particular sensitivity (for example, if it relates to those in sensitive professions such as lawyers, journalists, MPs, and ministers of religion), the public interest in the integrity of telecommunications or postal operators' systems, and any other aspects of the public interest in the protection of privacy must also be taken into consideration by the Secretary of State.

The operation of the communications data retention regime is overseen by the Investigatory Powers Commissioner. Any operator given a notice can seek a review of that notice by the Secretary of State, who must consult the Commissioner and the Technical Advisory Board. Additionally, the Information Commissioner oversees compliance with requirements surrounding the security of retained data, and a complaint regarding communications data retention can be made to the Investigatory Powers Tribunal.

Therefore, in practice, taking into account all the matters that the Secretary of State must take into consideration, a data retention notice will target individual services and particular types of data offered by a given provider, and will stipulate the length of time for which different types of data must be retained. Section 90(13) of the Act requires the Secretary of State to keep a data retention notice under review, and revoke a notice where retention is no longer necessary and proportionate, or vary it where retention of communications data relating to a particular service offered by the provider is not necessary and proportionate. Law enforcement has engaged with over 700 telecommunications and postal operators in the past two years, less than 25 of these are or have ever been subject to a data retention notice.

Considering the necessity and proportionality considerations that must be taken into account, and the resulting practical effect of the regime to limit data retention by telecommunications operators or postal operators, services and data types, we do not consider that the existing data retention regime is 'general and indiscriminate'. It currently provides that data retention is based on objective criteria.

Nevertheless, we consider it important that the data retention regime is clear and transparent. Accordingly, we propose to amend the current regime so that the list of factors that the Secretary of State must take into account when giving a data retention notice to a telecommunications operator or postal operator under section 88 of the IPA will:

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

Restriction to serious crime

> *Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure. [para. 102]*

The judgment requires that where traffic and location data are retained or acquired for the purpose of the prevention or detection of crime, this should be restricted to 'serious crime'. The judgment does not seek to define serious crime, and it is the Government's position that the definition of serious crime for such purposes is a matter for EU Member States to determine within the context of national legal systems.

In its present form, the IPA permits the retention of and access to data for 10 purposes. The Government considers that communications data should not be retained or acquired

for trivial matters, and the important tests of necessity and proportionality in the Act prevent data being retained or acquired where it is not appropriate to do so. Nevertheless, the Government proposes to amend the Act to impose a serious crime threshold in relation to the retention and acquisition of events data for criminal purposes.

The proposed amendments to the legislation provide a definition of 'serious crime' for the purposes of the retention or acquisition of events data, which will apply to investigations into all offences for which an adult is capable of being sentenced to six months or more in prison; any offence involving violence; any offence which involves a large number of people acting in pursuit of a common purpose; any offence committed by a body corporate[1]; any offence which involves the sending of a communication or a breach of privacy; or any offence involving a significant financial gain.

UK law contains a variety of different definitions of serious crime, which are specifically designed to be relevant to the particular statute or power to which they relate. The definition of 'serious crime' we are proposing differs from the general definition of 'serious crime' in the IPA in the following respects:

(1) The general definition of "serious crime" in section 263 of the IPA applies to conduct for which an adult could reasonably be expected to be sentenced to three years or more in prison;
(2) The general definition does not include any offence committed by a body corporate, or any offence which involves the sending of a communication or a breach of privacy.

When developing the definition of serious crime for these purposes, we have been mindful of the points set out below, which have led us to consider that using the existing serious crime threshold in the IPA would significantly undermine the utility of communications data in the prevention or detection of crime, and create major difficulties for law enforcement agencies ("LEAs").

The existing serious crime threshold in section 263 of the IPA is a high threshold and excludes a wide range of offences where it would be appropriate to be able to acquire communications data (for example, harassment and grooming). These crimes can often escalate into more serious offences and communications data may be the only avenue to investigate online activity.

During the passage of the IPA, we worked closely with LEAs to consider the importance of obtaining communications data against a range of offences, with a particular focus on cases where it was anticipated that communications data will be an important, or indeed the only, investigative tool.

Key offences highlighted by law enforcement, include:

- Harassment and grooming offences – where there are various offences with a sentencing maximum of 6 months and some lesser offences punishable by a fine. Where the activity takes place online, communications data may play a key role in the investigation. Such activity can often escalate into more serious offences. Concerns have been raised in Parliament about the police response to harassment.

[1] A body corporate is an organisation such as a company or government body that is considered to have its own legal rights and responsibilities.

We do not consider that privacy concerns should prevent the use of investigatory powers to protect individuals from abuses of their privacy by criminals.

- Using, disclosing and acquiring data for an unauthorised purpose – these offences under the Data Protection Act 1998 are only punishable by a fine. They are intended to protect privacy and where data is disclosed online, communications data could be critical to identifying the culprit. These offences can often have serious consequences for the victims - for example, where private financial records are stolen.

Moreover, serious corporate offences such as corporate manslaughter do not attract custodial sentences.

The importance of being able to use communications data to investigate the above offences explains why the Government proposes to impose a 6 month rather than 3 year threshold for serious crime in this context, and to include offences committed by a body corporate, or which involve the sending of a communication or a breach of privacy.

The Government also considers that there is good reason for applying a test that an adult should be “capable” of being imprisoned for 6 months in this context, rather than a higher threshold test that they may “reasonably expect” to be imprisoned for the requisite period (as in section 263 of the IPA). The higher test in section 263 is workable in an interception context, as the types of crimes for which interception powers are used are ones where the sentence would easily surpass the “period” threshold of 3 years. So the number of cases in which the public authority would need to carefully consider whether the threshold is met is low. In the communications data context, public authorities will often be working much closer to the “period” threshold, and considering likely sentencing before making a request would significantly add to the complexity of the regime. Moreover, communications data may be of particular use at an early stage in an investigation, at which point the seriousness of the offence concerned may not be fully known.

Additionally, we propose to remove three of the statutory purposes for which data can currently be retained or acquired, namely:

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

The Act allows for the retention and acquisition of communications data for a number of purposes which extend beyond the prevention and detection of criminality. These three purposes which we propose removing could allow for communications data to be retained or acquired in relation to criminal activity that would not meet the serious crime threshold.

Retention safeguards

Security of retained data

> *Guarantee a particularly high level of protection and security of data by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period [para. 122]*

As a minimum requirement, section 92 of the IPA ensures that data is retained to at least the same level of security as on any system from which the data is derived, and also requires providers to put in place technical and organisational measures to ensure the data can only be accessed by authorised personnel and to protect against accidental or unlawful loss, processing, access or disclosure.

Security, be that physical (buildings, CCTV, etc.), technical (e.g. firewalls and anti-virus software), personnel (such as staff security vetting and training), or procedural (e.g. processes and controls), is a consideration for the Secretary of State whenever data retention notices are considered or new arrangements are put in place, and retention systems are built to meet stringent security requirements and are subject to compliance checks by accredited security experts. Oversight of these arrangements is provided by the Information Commissioner.

Additionally, under section 87 of the Act, a retention notice may specify any other requirements in relation to the retention of data. This can be used to impose specific requirements in relation to data security, such as requiring a provider to conduct a security audit of their systems.

The Government considers that it would not be appropriate to make further provision on security on the face of the legislation, as levels of security depend on a number of different factors, which are set out in the draft code of practice. In addition, communications data varies in its levels of intrusiveness, so a ‘one size fits all’ approach will never be appropriate.

Telecommunications operators and postal operators are also required to comply with relevant data protection legislation, the requirements of which include ensuring the appropriate security of data.

Where a telecommunications operator or postal operator generates or processes data within the EU it must be held in compliance with EU data protection legislation. In particular, transfers outside the EU are permitted only where the recipient can provide an adequate level of protection for that data, or in other limited circumstances. We do not consider that the judgment was seeking to restrict transfers of data where the requirements of EU law are met. The eighth data protection principle states “*personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data” and* amendments have been made to the code of practice to make clear how the principle applies to retained communications data.

The IPA allows the Secretary of State to give a data retention notice to any company providing a service to UK customers wherever that company is based. Accordingly, a data retention notice may be given to an operator whose data is not held in the EU. Even some EU-based companies may hold their data abroad. Transferring data internationally without good reason would introduce unnecessary risks to the data and therefore we do not consider that the CJEU can have intended to require data which is generated, processed or stored securely outside the EU to be transferred into the EU to be retained. Having regard to the importance of data being retained securely, we have nevertheless included additional proposed requirements in the code of practice which will ensure that where data is held outside the EU, it is retained to an adequate level of protection, comparable to that required by EU data protection laws. We invite comments, in particular from telecommunications and postal operators, on our proposed approach to data security and data held outside the EU.

Access safeguards

Independent authorisation of requests to access communications data

> *It is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime [para. 120]*

The CJEU's judgment is clear that requests to acquire retained communications data must be approved by a court or independent administrative body, and the Government has accepted in the domestic courts that access to retained data must, in most cases, be subject to prior independent approval.

The draft Regulations amend Part 3 of the IPA to provide for three different regimes for authorisation of communications data requests:

Independent authorisation

The draft Regulations create a new power for the Investigatory Powers Commissioner (IPC) to authorise communications data requests. The IPC will delegate these functions to a newly appointed body of staff, to be known as the Office for Communications Data Authorisations (OCDA). OCDA will report directly to the IPC, and will be responsible for considering the vast majority of requests to access communications data made by public authorities.

The Government is working to establish ODCA in consultation with the IPC and the task of setting it up is significant. It involves the procurement of premises (including appropriate security arrangements), recruiting and training new staff, and the development of the necessary IT systems and processes which will allow OCDA staff to electronically consider applications from over 600 public authorities.

At present, the IPA requires local authority applications to be subject to judicial approval by a magistrate. The draft Regulations remove this requirement. The Government considers

this provision is unnecessary in the light of the new independent arrangements, and retaining it would undermine the role of OCDA. However, recognising the need to ensure that local authorities use their powers appropriately, the code makes clear that senior internal approval is required before an application is sent to OCDA for authorisation.

Internal authorisation for urgent cases

The judgment recognises that it is acceptable to authorise requests internally in cases of validly established urgency. Accordingly, the new regime will allow for internal authorisation by a designated senior officer in a public authority where there is an urgent need to obtain communications data.

Authorising urgent requests internally will be available to all public authorities except local authorities, who will be prohibited from authorising communications data requests internally for any purpose.

Internal authorisation in other cases

As set out above, the Government's position is that the judgment does not cover requests for communications data made for national security purposes, and we are therefore maintaining the current internal authorisation regime for these cases. Where a public authority may make a request for the purposes of national security or the economic well-being of the UK, where linked to national security (set out in Schedule 4 to the Act), these cases can be authorised by a designated senior officer within the public authority. As now, these designated senior officers will need to be independent of the investigation except in the limited circumstances currently defined in the Act.

As law enforcement bodies will be making the vast majority of their communications data applications to OCDA, they may choose, for practical purposes, to direct their national security applications through OCDA too. However, it will be open to public authorities to authorise national security applications internally, in accordance with existing procedures, should they wish to do so.

As explained above, the work of the three UK intelligence agencies – MI5, MI6 and GCHQ is out of the scope of EU law, and accordingly they will continue to authorise the vast majority of their applications for communications data internally.

As set out above the government considers that entity data is outside the scope of the judgment. However, at present we judge that providing for all communications data applications for entity data to be subject to internal authorisation would make the regime unnecessarily complex and under the Government's proposals requests for entity data will be authorised in the same way as requests for events data.

Notification

> *The competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is…necessary to enable to persons affected to exercise…their right to a legal remedy… [para. 121]*

The requirement in the CJEU's judgment for *ex-post* notification is based on the underlying principle that those who have been the subject of investigatory powers should have effective access to a right of redress where this may have been done unlawfully. In the UK, the Investigatory Powers Tribunal provides such a right of redress. Any person who believes that investigatory powers have been unlawfully used against them can make a complaint to that Tribunal. A person making such a complaint does not need to know whether, or demonstrate that, any powers have actually been used.

The Government's position is that a general requirement to notify an individual that their data has been accessed would unnecessarily inform criminals, suspected criminals and others of the investigative techniques that public authorities use. Simply because an investigation has ceased or an individual is ruled out of a particular investigation does not mean that notification would not be operationally damaging. Criminal networks and investigations are much more complex than this. For example:

- A public authority may acquire the data of someone who is a victim of a crime to corroborate their claim. While it could be thought appropriate to notify the victim of a crime that their data has been obtained, there are examples where people who were thought to be victims turn out, at a later date, to be involved in the criminality. If they were informed that their data had been acquired, they may become more cautious with their communications and their involvement in criminal behaviour may never be determined.

- An individual whose communications data has been acquired as part of an investigation is subsequently discounted from the inquiry and notified that their communications data has been acquired. That individual goes on to reveal this fact to associates who are involved in the crime, thus alerting them to the investigation.

- Where communications data is used to locate a vulnerable missing person, notifying them that their communications data (such as location data from their mobile phone) was acquired to locate them could cause them to take action in the future, such as not taking their phone with them, which will close an avenue used to locate them safely.

Additionally, there are real challenges posed by the number of different authorities who are able to use these powers, and de-conflicting everyone involved in one investigation with all other investigations run by all public authorities, including the security and intelligence agencies, would be practically impossible. It is possible that one person may be of interest in different investigations carried out by different public authorities, and if one public authority notified a subject once their investigation has ended, it could fatally undermine investigations by other public authorities. Clearly, some investigations are very sensitive, and it would be impossible to fully mitigate this risk across different organisations.

The Government considers that the existing regime under the IPA provides sufficient scope for notification through a variety of mechanisms. For instance, the Investigatory Powers Commissioner can notify a person if a serious error occurs (paragraph 24.33 of the draft communications data code of practice explains what a serious error is).

The draft code of practice also requires that when public authorities acquire communications data, they must specify whether the application can be disclosed to the individual whose data was acquired.

Separately, the criminal justice system provides for notification where the data acquired is used as evidence. A defendant is notified that their communications data has been acquired unless a judge agrees that disclosure of that information would not be in the public interest. Obligations under the Criminal Procedure and Investigations Act 1996 also provide that the prosecution must disclose material which undermines the prosecution case or assists that of the defendant.

The Government's current position, accordingly, is that our regime already provides for sufficient notification of individuals where appropriate, and is consistent with requirements under the ECHR. We consider that imposing greater notification obligations in the circumstances set out above would damage investigations. We invite comments on this approach, as part of this consultation.

Glossary of terms used in this consultation and associated documents

Subscriber data – defined in RIPA as information held or obtained by a communications service provider about persons to whom they provide or have provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it. The IPA defines this data as a type of 'entity data'.

Entity data – defined in the IPA as information about a person or thing, and about links between a telecommunications service, part of a telecommunication system and a person or thing, that identify or describe the person or thing. For example, individual communication devices such as phones, tablets and computers are entities, as are the links between a person and their phone, which would include billing payments, who the account holder is, and information about apparatus or devices used by, or made available to, the subscriber or account holder.

Traffic data – defined in the ePrivacy Directive as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data includes data relating to the time a telephone call was made, to which number, and the duration of the call.

Location data – a term defined in the ePrivacy Directive as any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. For a landline, it will be the fixed location of that apparatus, whilst for a mobile telephone it will be the cell mast the call was made from.

Events data – defined in the IPA as including information about time-bound events taking place across a telecommunication system at a specific time, and combines the categories of traffic and location data from RIPA, as described above. This includes information which identifies, or appears to identify, any person, apparatus or location to or from which a communication is transmitted.

Telecommunications operator – a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (in whole or in part) in or controlled from the UK.

Postal operator – a person providing a postal service to a person in the UK.

Serious error – an error made by a public authority when complying with any requirements imposed on it by virtue of the IPA, which the Investigatory Powers Commissioner considers has caused significant prejudice or harm to the person concerned.

© Crown copyright 2017

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

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

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

DRAFT