Home Office

Investigatory Powers Act 2016:

Response to Home Office 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

JUNE 2018

This publication is available at www.gov.uk

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

Contents

Introduction 4

Consultation Responses 6

- Table of respondents 6

Principal comments and proposed changes 7

- Application of the judgment to national security 7
- Application of the judgment to entity data 7
- Independent authorisation 8
- Restriction to serious crime 9
- Scope and permissibility of the regime 10
- Security of retained data 10
- Notification 11
- Comments on the code of practice 12
- Representations received outside of the scope of this consultation 13

Next steps 14

Introduction

The Investigatory Powers Act 2016 (IPA) provides that telecommunications and postal operators may be required by the Secretary of State to retain communications data – the who, where, when, how and with whom of a communication, but not what was written or said – for up to 12 months, where it is considered necessary and proportionate to do so, and where the decision to impose such a requirement has been approved by a Judicial Commissioner. Specified public authorities may acquire communications data from a telecommunications operator or postal operator where it is both necessary and proportionate to do so, for specified purposes.

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 and local authorities of this vital tool. From January to December 2015, 761,702 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. 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.

In December 2016, the Court of Justice of the European Union (CJEU) handed down its judgment in two joined cases, one of which was a reference from the Court of Appeal relating to a challenge to the Data Retention and Investigatory Powers Act 2014 (DRIPA). DRIPA was the legislation governing the retention of communications data prior to the commencement of Part 4 of the IPA.

The CJEU ruled 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 the requirements of EU law.

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.

In light of the importance of communications data as an investigative tool used by those responsible for keeping citizens safe, and after careful consideration of the CJEU's judgment, the Government proposes making amendments to the IPA.

This is a matter of public importance, and so the Government launched a public consultation on these proposed amendments on 30 November 2017. At the same time, the Government published the draft communications data code of practice for consultation. The consultation closed on 18 January 2018 and we have given detailed consideration to the responses, alongside the relevant Court of Appeal and Divisional Court judgments handed down in January 2018 and April 2018 respectively.

We are grateful to those who took the time to consider the amendments and respond to the consultation.

This document provides an overview of the representations received during the consultation period and the Government response to them, and outlines the changes that will be made as a consequence of these comments, and the next steps.

Consultation Responses

We received 794 responses to the public consultation, of which 716 were a direct result of a campaign run by the digital campaigning organisation Open Rights Group, which encouraged its supporters to submit their views based on areas of concern expressed by Open Rights Group. The remaining 78 submissions were made by academics, members of the public, legal representatives, public authorities, telecommunications and postal operators, media groups, oversight bodies and civil liberties groups.

In addition to these responses, the campaign group 38 Degrees hosted a petition on its website which received 121,324 signatories. The petition text, addressed to the Home Secretary, read *"Please protect our privacy. Make the proposed amendments to the Investigatory Powers Act and comply with European Court of Justice ruling"*. It is unclear whether the signatories to this petition were supportive of the Government's proposals, which the Government considers are consistent with the ruling.

The consultation complied with all aspects of the Cabinet Office consultation principles.

Table of respondents

The following table lists the responses that were received during the consultation.

Type of respondents	**Number of responses**
Open Rights Group campaign respondent	716
Members of the public	56
Oversight bodies	2
Public authorities	4
Academics	2
Telecommunications and postal operators and industry bodies	5
Media groups	5
Civil liberties groups	4

Principal comments and proposed changes

Having given careful consideration to the representations received during the course of the consultation, we intend to make some changes to the proposals published for consultation. These changes will be both to the regulations and the code of practice, and whilst some are minor and typographical changes, others are more substantive. Further details of where we intend to make these changes are provided below.

During the course of the consultation, we also received representations on a number of issues that did not fall within the scope of the consultation, for example the bulk powers provisions in the IPA, and the Government's position on the use of encryption. Further detail of these broad themes are also provided below.

Application of the judgment to national security

A small number of respondents opined that the requirements of the judgment should apply to applications made for national security purposes.

As outlined in the consultation document, the Government position is that the judgment does not apply to the retention or acquisition of communications data for national security purposes, as the CJEU may only act within the limits of the competences conferred upon the EU by the Member States in the EU Treaties, and Article 4(2) of the Treaty of the European Union explicitly identifies national security as being the sole responsibility of Member States. Indeed, the consultation document explains that this issue is subject to a pending reference to the CJEU in proceedings before the Investigatory Powers Tribunal. More recently, the High Court refused to make a further referral to the CJEU on this same matter. For these reasons, this issue is outside the scope of the consultation.

Application of the judgment to entity data

As outlined in the consultation document, 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 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.

Of the small number of respondents who provided thoughts on the applicability of the judgment to entity data, the majority agreed with the Government position outlined in the consultation document. For those who did not agree, it is important to recognise that the Government's position is not one that has a significant material impact on the regime. For the purposes of authorisation, the Government will be treating entity and events data in the same way, which will mean that independent authorisation will be required. With regards to serious crime, although the legislation will permit entity data to be retained and acquired for non-serious crime, the requirement for necessity and proportionality means that entity data

will only be retained or acquired in such circumstances where the strict tests of necessity and proportionality are met.

Indeed, the High Court recently concluded, in its judgment on the challenge to Part 4 of the IPA, that *"the definition of events data under the 2016 Act embraces both location data and traffic data in the e-Privacy Directive and so entity data under the 2016 Act does not fall within the scope of [the CJEU judgment]".*

Some respondents suggested changes to the regime which would require changes to the Act, voicing concerns that the safeguards already provided in the Act and code of practice would not be adhered to. The role of this code of practice is to set out how public authorities and telecommunications and postal operators apply the provisions in the Act. It is not the role of the code of practice to seek to limit the scope of the powers. Nor can the code go further than the Act in the conduct that is permitted. It is important to remember that the Investigatory Powers Commissioner, in his oversight of the communications data regime, is a key safeguard to ensure all the requirements of the Act and code are complied with by public authorities. One of the elements of his oversight is to ensure that the strict case for necessity and proportionality is met in all authorisations to access retained communications data. Additionally it is an offence under the Act for a person in a relevant public authority to knowingly or recklessly to obtain communications data from a telecommunications or postal operator without lawful authority.

Independent authorisation

Our proposal to create a new power for the Investigatory Powers Commissioner to authorise communications data requests, and the consequent creation of the Office for Communications Data Authorisations (OCDA), was met with broad approval by all those who commented on it in their consultation responses.

There was misunderstanding amongst some respondents that the creation of OCDA would replace the post-authorisation oversight function provided by the Investigatory Powers Commissioner, which is not the case. Some calls were made for all communications data applications to be considered by the judiciary instead. As the CJEU judgment makes clear, these applications should *"be subject to a prior review carried out by a court or by an independent administrative body"*. It simply would not be feasible for the UK courts to process the number of applications for communications data made each year, and our proposals are clearly consistent with the requirements of the judgment.

A handful of responses commented on our proposals to allow for authorisation internal to the public authority in cases of validly established urgency, expressing concern that this is circumventing the terms of the judgment. As detailed in the consultation document, the judgment explicitly permits the internal authorisation of communications data requests "in cases of validly established urgency", and this therefore meets the requirement of the judgment. The amendments we are proposing to the Act mean that an authorisation made using the urgent internal process cease to have effect after 3 days, ensuring that a request must be made to OCDA where activity authorised internally via the urgency process is ongoing at the end of the 3 day period. We have now amended the code of practice to make this restriction on urgent applications clear. Of course the use of the urgency procedure also remains subject to the usual oversight by the Investigatory Powers Commissioner.

There was also some concern that the change to independent authorisation of requests would lead to the removal of the role of the SPOC (or single point of contact). The changes we are proposing only affect the authorisation of requests and SPOCs will retain their crucial

role between the applicant in the public authority and the relevant authorising officer. SPOCs will, in the vast majority of cases, continue to be the people who make requests for data to telecommunications and postal operators.

Restriction to serious crime

We received a number of responses to the consultation that were supportive of our proposed definition of serious crime for use solely in the communications data context, including the proposed removal of three statutory purposes. There was also recognition of the essential role communications data plays in a broad range of investigations, for instance domestic abuse cases, where offending may quickly escalate in terms of seriousness and risk of harm to the victim. However, the majority of respondents who commented on that proposal considered that an offence for which an adult was capable of being sentenced to six months imprisonment was not sufficiently serious to merit being described as 'serious crime', and therefore did not meet the requirements of the judgment.

Some respondents misinterpreted the existing regime, believing that all communications data requests must already be for serious crime purposes, and that our proposal would therefore lower the existing threshold. The Act currently permits communications data to be retained and acquired for the purpose of preventing or detecting crime or preventing disorder, rather than being restricted to serious crime. The intention we laid out in the consultation document is to introduce an additional serious crime threshold which is relevant solely in the context of the retention and acquisition of communications data. This remains our intention. It is recognised that communications data is a less intrusive capability than others provided for by the Act, such as interception of communications, and the types of investigations in which it plays a vital role can carry shorter lengths of prison sentence. As was stated in the consultation document, in some circumstances, such as where the criminality takes place online, communications data may be the only way to progress an investigation. This change does not affect the serious crime threshold for other powers in the Act as some respondents feared.

Respondents made suggestions for how the proposed serious crime definition could be tightened, for instance by defining the exact type of crimes covered, or by increasing the minimum prison sentences available for certain crimes to the three year threshold provided in section 263 of the IPA. It would not be right to inflate sentencing thresholds in this way, as each sentencing threshold should be an appropriate punishment for the crime, not appropriate to the use of a particular investigative technique. In addition to this, as sentencing for different crimes are set out in the relevant statutory framework, to increase the minimum sentences for each offence would require each piece of legislation to be amended. This is not a feasible approach.

We have, though, listened to the concerns expressed by respondents that our proposed serious crime threshold in the communications data context was too low.

Therefore in the regulations that have been laid before Parliament, we have increased the crime threshold for which events data can be acquired to crimes for which a person is capable of receiving 12 months in prison. This will means data cannot be acquired for the investigation of crimes where a person is not capable of being sentenced to 12 months imprisonment. Depriving a person of their liberty by handing down a prison sentence is, of course, a serious issue.

We also understand the concerns that respondents expressed about the broad spectrum of seriousness that could be captured within the serious crime definition we are proposing for

communications data acquisition. For example the offence of theft carries a maximum sentence of 14 years but also includes more low level offences such as shoplifting. To address such cases we have set out explicitly in the code of practice the considerations that must be addressed by public authorities when considering whether the crime is sufficiently serious to justify the acquisition of such data. This makes clear that relevant public authorities should also consider factors such as the particular circumstances of the case, the offender, the impact on the victim, the harm suffered, and the motive of the crime in order to demonstrate that the acquisition of communications data is proportionate.

Of course it will still only be possible to acquire communications data on a case-by-case basis, and only where the officer authorising the application considers that it is necessary and proportionate in that specific case. In the future this decision will, in the vast majority of cases, be made by the independent Office for Communications Data Authorisations once it is established.

One respondent was concerned that removing 'for the purpose of protecting public health' might affect the investigation of infectious diseases, including where there is a serious epidemic. The Government is content that in such circumstances where it is necessary and proportionate to acquire communications data, the 'purpose of preventing death or injury or any damage to a person's mental or physical health, or of mitigating any injury or damage to a person's physical or mental health' would be sufficient and that there will not, therefore, be damage to public health resulting from this change.

One respondent expressed concern at removing 'tax evasion from the list of reasons for the collection of data'. It is important to be clear that criminal offences relating to tax evasion attract a maximum sentence above the proposed 12 month threshold and therefore the removal of the tax purpose will have no impact on HMRC serious criminal investigations into tax evasion.

Scope and permissibility of the regime

There was general consensus amongst respondents that an EU Member State's data retention regime should not be general and indiscriminate, in accordance with the requirements of the CJEU judgment. For the reasons laid out in the consultation document, we believe that our existing regime meets the requirements of the judgment in this area, and we will be making no further amendments to our proposals in this respect.

In the recent challenge to Part 4 of the IPA, the High Court ruled that *"it could not possibly be said that the legislation requires, or even permits, a general and indiscriminate retention of communications data"*, rejecting the claim that it is inconsistent with EU law because it provides for the general and indiscriminate retention of communications data. The High Court was therefore clear that the existing regime is consistent with EU law in this regard and is not general and indiscriminate.

Security of retained data

The Government position on the transfer of data generated, processed or stored securely outside the EU, namely that it is not required to be transferred to the EU to be retained, was supported by a number of respondents who expressed a view on the matter. Some respondents raised concerns about the sharing of data with overseas partners, with some calling for no data to be shared overseas, whilst others asked that the precise safeguards required to be in place before such sharing could occur were contained within either the

legislation or the code of practice. As noted in the consultation document, where a telecommunications or postal operator generates or processes data within the EU, it must be held in compliance with EU data protection legislation, which permits the transfer of data outside the EU where the recipient can provide an adequate level of protection for that data, or in other limited circumstances. Our regime is consistent with these requirements, and those industry bodies who responded to the consultation supported this position.

There were some general concerns expressed around the security of the retained data, and that it might prove a target for hackers. Telecommunications and postal operators have to comply with the Data Protection Act 2018 and the Privacy and Electronic Communication Regulations 2003, the requirements of which include ensuring appropriate security of data. In addition, they are required to comply with the requirements of the IPA, as well as any specific security requirements stipulated in a data retention notice served on them. The code of practice also sets out further details on security of retained data. The Information Commissioner audits the compliance with security requirements for data retained by telecommunications and postal operators and its destruction at the end of the retention period. The Commissioner also enforces the security requirements in the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003, including by using the power to impose monetary penalties for serious contraventions. The Government is, therefore, confident that these requirements ensure retained communications data is held securely.

One respondent expressed concern that the code of practice does not provide minimum standards for the security of data retention systems. There are in fact minimum standards insofar as the Act requires data to be retained to at least the same standard as the system from which it is derived. The code has been amended to reflect this. However, that is, of course, a minimum standard and the code also reflects the other considerations which will usually result in additional data security protections being attached to the data. It is right that security of data is considered on a case by case basis to ensure that the level of protection applied is appropriate in all circumstances.

Notification

As set out in the consultation document, the Government has been clear 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. As some of the respondents to the consultation acknowledged, the fact that an investigation has ceased or an individual is ruled out of a particular investigation does not mean that notification would not be operationally damaging elsewhere. However, the Government has been clear that our position does not mean that individuals are never notified that their data has been accessed. Indeed there are already mechanisms (which are specified in the code of practice) by which individuals can be notified. For example, the Investigatory Powers Commissioner can notify people of serious errors and highlight their route of redress through the Investigatory Powers Tribunal. Where it would not be damaging to investigations, the public authority may also allow the telecommunications operator to notify the individual, for example when the telecommunications operator receives a subject access request under data protection legislation. And when communications data has been acquired during the course of a criminal investigation that comes to trial an individual will be made aware, in most cases, that data has been obtained.

Several respondents considered that notification is a valuable safeguard for an individual to be told about their involvement in an investigatory powers request and, whilst the majority of those making comment on this issue said that this should happen in all instances, others

acknowledged that it could happen provided that to do so would not have any adverse impact on ongoing operations.

This issue remains subject to ongoing litigation, and the Government's position remains that our regime already provides for sufficient notification of individuals where appropriate, and is consistent with requirements under EU law and the European Convention on Human Rights.

Comments on the code of practice

A number of comments were received on areas of the code of practice not covered above. A number of respondents, in particular media groups, requested further clarity on the definition of journalists and their sources. Responses from journalist groups also requested additional language on the importance of protecting sources and Article 10 rights. During the earlier public consultation on the other IPA codes we received similar representations on this subject and these were carefully considered at the time. We have been mindful of those comments when considering responses received during this consultation. It is important that the language in the code of practice is consistent with the Act and, where relevant, with the other codes of practice which sit under the Act. It would be undesirable for public authorities to operate to different guidelines relating to journalists depending on the power that they are using.

There was some concern that the request filter should not be used to process large quantities of data. The request filter provisions in the IPA were subject to significant debate during the passage of the legislation and the code should not be used to artificially limit the scope which Parliament has approved in primary legislation. The Government is confident that the code is already sufficiently clear that the filter is a safeguard that will be used to limit the amount of data that needs to be disclosed by relevant public authorities. However, we have made a number of amendments to make clear that public authorities 'must' fully consider proportionality in using the filter. The filter is subject to oversight by the Investigatory Powers Commissioner who will be consulted on the types of processing that the filter can carry out.

A number of respondents suggested there should be clearer record keeping requirements for novel and contentious requests. The draft code was already clear that records must be kept, however we have also made this clear in the record keeping section of the code.

There were some responses which sought clarification that retained data will not be available to be acquired by all public entities. The Government can confirm that is the case and only those 'relevant public authorities' that are set out in Schedule 4 to the Act can exercise the power to acquire retained data. A small number of respondents queried the types and number of public authorities empowered under the Act. The Government keeps under constant review the number of public authorities which can acquire communications data, and only organisations that are able to demonstrate a compelling need are provided with the power. It is worth noting that the Home Office undertook a review of all public authorities during the passage of the Act, and those listed at Schedule 4 to the Act are those who demonstrated a requirement to be able to obtain communications data in order to fulfil their statutory obligations. During the passage of the Act the government published a document setting out the case for such public authorities to have access to communications data. This can be found at the following link:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/536331/operational-case-for-the-use-of-communications-data-by-public-authorities.pdf.

A number of responses raised internet connection records and their scope. It is important to be clear that this is a new power that Parliament approved and the code of practice sets out what is likely to be covered by the power. As set out above it is not possible for the code to extend the power beyond what is provided for in the legislation, nor should it be used to restrict the power approved by Parliament.

In addition to those areas covered above a number of small drafting changes were made in response to comments to improve clarity of the requirements contained in the code.

Representations received outside of the scope of this consultation

Along with views on the issues above, we also received representations on elements of investigatory powers and other issues falling outside the scope of the consultation.

Subjects covered included a general opposition to powers provided for in the IPA (including the cost of implementing the powers) as well as more specific provisions, such as the exclusion from legal proceedings of material obtained by virtue of an interception warrant, and monitoring techniques such as police use of facial recognition technology, automatic number plate recognition technology, and corporate use of data. We do not propose to comment on this broad range of issues that were out of scope of the consultation.

Next steps

The regulations and code of practice have been laid before Parliament for approval. They will only come into force once they have been debated in both Houses of Parliament and each House has expressly approved them.