Regulation of Investigatory Powers Act

Response to Public Consultation: Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice

March 2015

Introduction & the legislation

Communications data – the 'who, where, when and how' of a communication but not its content – is a crucial tool for fighting crime, protecting children and combating terrorism.

Communications data is collected by the communications industry for their own business purposes. This data can be retained by communication service providers (CSPs) under the Data Retention and Investigatory Powers Act 2014 (DRIPA) which provides a clear basis on which domestic companies can be required to retain certain types of communications data. CSPs may also retain data in accordance with the voluntary Code of Practice under the Anti-Terrorism Crime and Security Act 2001. DRIPA and the Data Retention Regulations 2014 made under it replaced the UK's previous data retention regime following a European Court of Justice ruling in April 2014. That judgment ruled that the EU Data Retention Directive was invalid and DRIPA was enacted in part to put the basis for retention in the UK beyond doubt.

The Counter-Terrorism and Security Act 2015 (CTSA) amended DRIPA, in addition, to provide for the retention of data to enable a CSP to determine which device had been used to send a communication on the internet (known as IP resolution).

Under the Regulation of Investigatory Powers Act 2000 (RIPA), law enforcement, the intelligence agencies and other relevant public authorities can seek access for certain statutory purposes (such as the prevention or detection of crime) to the communications data held by communications service providers if they can demonstrate that access is necessary, proportionate, and is connected to a specific investigation or operation.

Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade and has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service. It has played a significant role in the investigation of many of the most serious crimes in recent times, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman and the murder of Rhys Jones. It can prove or disprove alibis, it can identify associations between criminals, and it can tie suspects and victims to a crime scene.

The codes

The new Data Retention Code of Practice sets out how the Government implements the requirements in DRIPA, as amended by the Counter-Terrorism and Security Act, and in the Data Retention Regulations. It covers the issue, review, variation and revocation of data retention notices, the CSPs' ability to recover their costs, data security, oversight by the Information Commissioner and safeguards on the disclosure and use of retained data by CSPs.

The amended Acquisition and Disclosure of Communications Data Code of Practice updates, clarifies and provides guidance on the safeguards and procedures regarding the acquisition and disclosure of communications data by public authorities under RIPA. The acquisition code sets out rules for the grant of authorisations to acquire data, the giving of notices to require disclosure of data and the keeping of records, including records of errors.

Consultation

On 9 December 2014 the Home Office launched a consultation on proposals to update the Acquisition and Disclosure of Communications Data Code of Practice and publish a new Retention of Communications Data Code of Practice, following the passage of DRIPA and the Data Retention Regulations in July 2014.

The acquisition code was last published in 2007 and we have made a number of clarifications and updates to bring the code in line with current approaches and processes, reflecting the experience of public authorities in using the code. We have also made a number of changes to the acquisition code following the European Court of Justice judgment and recommendations by the Interception of Communication Commissioner.

The key changes are

- enhancing the operational independence of the authorising officer from the specific investigation for which communications data is required;
- ensuring that where there may be concerns relating to professions that handle confidential or privileged information (e.g. lawyers or journalists), law enforcement should give additional consideration to the level of intrusion and must record such applications;
- reflecting the additional requirements on local authorities to request communications data through a magistrate, and the National Anti-Fraud Network;
- setting out new record keeping requirements for public authorities; and
- aligning the code with best practice regarding responses to public emergency calls (999/112 calls) and judicial co-operation with overseas authorities.

Around 300 replies were received, of which approximately 250 related wholly or primarily to the issue of access to the communications data of journalists.

This document is the summary of, and response to, the comments received during the consultation. It considers the responses in five sections:

- Those relating to the UK's communications data regime;
- Those relating to both codes of practice;
- Those relating to the data retention code of practice;
- Those relating to the acquisition and disclosure code of practice; and
- Those relating to the issue of access to the communications data of journalists.

Comments relating to the UK's communications data regime

A number of responses commented on the legislative framework for either data retention or acquisition in the UK. The key concerns raised were:

The scope of RIPA

Comments:

A number of respondents commented that RIPA was terrorism legislation and should not be used beyond terrorism and serious crime. A smaller number commented that there was no distinction made between the communications data of serious criminals and others not suspected of crimes. Comments were also received suggesting that too many public authorities had access to communication data under RIPA.

Response:

It is not the case that RIPA is, or has ever been, 'terrorism legislation' – it governs the use of investigatory powers by public authorities in a wide range of contexts. Section 22 (2) of RIPA sets out the purposes for which communications data can be acquired by public authorities and further purposes can be found in the Regulation of Investigatory Powers Act (Communications Data) Order 2010, as amended by the Regulation of Investigatory Powers Act (Communications Data) (Amendment) Order 2015. These purposes, which have been approved by Parliament, are broader than the prevention and detection of serious crime and include public safety, the collection of taxes and preventing death or injury.

Section 22 (5) of RIPA sets out the public authorities which can acquire communications data. Further public authorities are listed in the Regulation of Investigatory Powers Act (Communications Data) Order 2010, as amended. The Regulation of Investigatory Powers Act (Communications Data) (Amendment) Order 2015 removed the powers from 13 public authorities.

The ability of these authorities to access communications data has been agreed by Parliament and the Orders limit what types of data authorities can access, for example local authorities do not have access to the most intrusive category of communications data and in practice most of their requests are for subscribers to mobile telephones. These authorities have demonstrated a legitimate need to access communications data and use it to investigate crimes such as trading standards offences and benefit and council tax fraud. Such crimes can have a significant impact on local communities.

Communications data is also required for legitimate purposes beyond the prevention and detection of crime. For example, it is used to track and find missing and vulnerable persons. In all circumstances, the application must lay out the considerations of why the applications is both necessary and proportionate – clearly the considerations are different when the data is for someone suspected of a serious crime and someone who is not suspected of any criminality. The new code provides additional guidance on necessity and proportionality.

The independent Interception of Communications Commissioner, in his 4 February report, wrote that it is "unhelpful when the reports in the media misinform the public by stating the use of powers to acquire communications data for crimes, not deemed to be of a serious nature under the Act, are inappropriate. It is also wrong for the reports in the media to cite the Act as a terrorist law and infer that its use for non terrorist related matters is inappropriate." (paragraph 6.8).

DRIPA and the ECJ judgment

Comments:

A number of responses were concerned that the legal framework did not take specific account of the European Court of Justice judgement in April 2014 which struck down the European Data Retention Directive. Respondents questioned in particular whether the legislation allowed for blanket retention of data.

Response:

There are well established safeguards and requirements in existing legislation to ensure that communications data can only be retained or acquired when it is necessary and proportionate to do so and which do not allow for indiscriminate or blanket retention.

During the passage of the Data Retention and Investigatory Powers Act last summer the Government published a document setting out its response to the concerns raised in the European Court of Justice judgment. This can be found on the GOV.UK website at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/331106/DRIPgovernmentNoteECJjudgment.pdf

Comments:

Some respondents commented on the territorial extent of data retention.

Response:

DRIPA provides for the retention of communications data that is generated and processed in the UK. It does not apply to services provided to the UK where the communications data relating to that service is generated and processed abroad.

Comments:

One respondent queried why the retention period for subscriber data commences at the point at which a customer leaves the service or at the point that a change is made, noting that this could mean that the data is retained for over 12 months since its creation.

Response:

The differences in retention period between subscriber information and other types of communications data reflect the different nature of the data. Traffic and service use data are records generated at a single point in time and the retention period commences immediately. As subscriber data remains current until such point as it is changed or would otherwise be deleted, the retention period only commences once the data is changed or the customer leaves the company.

The IP address resolution provisions in the Counter Terrorism and Security Act 2015

Comments:

Respondents queried the extent of these provisions and believed there should be more clarity on what data could be retained, including about a person's internet usage.

Response:

As noted above, the provisions in the CTSA mean that a CSP can be required to retain data to determine which device had been used to send a communication on the internet (known as IP resolution). The way in which CSPs build and run their systems varies and so the precise information they would need to resolve an IP address may vary between CSPs. Accordingly the data to be retained under a notice given to a particular provider would depend on the nature of the communications and the communications service being used. It may include port numbers (akin to a house number where an IP address is akin to a post code); media access control addresses (the identifier of the particular computer); and the time and the location. However, the provision specifically excludes the retention of data commonly known as web logs – which would identify which communications services or websites are being accessed over the internet by an individual device.

Comments:

Respondents raised concerns that the provisions meant that, for the first time, data would be retained which CSPs did not retain for business purposes and, further, that the processing of data by CSPs was a stepping stone to a central database.

Response:

DRIPA and the preceding legislation provided for the retention of data that was generated or processed by a CSP as part of providing a service. There has never been a requirement for a CSP to retain data for business purposes before it can be retained further. In light of the increasing complexity of internet communications, the requirements in the code in relation to the accessibility and processing of the data make clear that data carried in the core of the networks can be retained under the legislation and can, where appropriate to do so, be processed to ensure that data is only retained where truly necessary.

Comments:

One respondent raised concerns that the costs of implementing the provisions were likely to be higher than set out in the impact assessment which accompanied the Act.

Response:

The Home Office discussed the provisions with the CSPs likely to be affected both leading up to and during the passage of the legislation and these discussions informed the content of the impact assessment. We continue to discuss implementation with the service providers concerned and assess that the figures are an accurate representation of the expected costs.

The need for future legislation

Comments:

Some respondents felt that there needed to be a wider public debate on these issues with respondents considering that the codes of practice and indeed the law would not keep up with the pace of change in the communications industry. One group of respondents suggested particular means that might improve police access to communications data.

Response:

Communications technologies are changing fast and the increasing prevalence of internet communications means that communications data is not always available when it is needed. When the Prime Minister announced the introduction of DRIPA in July 2014 he made clear that he wanted it to be the start of a wider public debate on this issue. DRIPA contains a sunset provision to repeal it on 31 December 2016. Therefore, the legal framework concerning the retention of communications data will need to be reviewed again by Parliament before then.

David Anderson QC, the Independent Reviewer of Terrorism Legislation, is currently conducting a statutory review of investigatory powers, and is due to complete his review by 1 May 2015 and report to the Prime Minister as soon as reasonably thereafter. We will therefore need to return to this issue in the next Parliament, to ensure that our law enforcement and intelligence agencies maintain the capabilities they need to protect the public and keep us safe.

Other

Comments:

There were concerns that the Interception of Communications Commissioner is not sufficiently resourced to carry out his role.

Response:

The acting Interception of Communications Commissioner confirmed, to the Home Affairs Select Committee on 4 November 2014, that he considers that the Interception of Communications Commissioner's Office has sufficient resources to carry out its functions.

Comments relating to both codes of practice

Combined code of practice

Comments:

One respondent suggested that one single code should be produced, covering both the retention and acquisition of communications data, in order to avoid duplication.

Response:

It was not appropriate at this stage to combine the codes, since the statutory powers which underpin the retention code expire at the end of 2016.

Costs

Comments:

Some respondents were keen to ensure that CSPs were repaid 100% of their costs in relation to data retention requirements.

Response:

The legislation provides for appropriate contributions to be made to CSPs.

Comments relating to the retention code of practice

There were a limited number of responses covering the retention code of practice or the addendum in relation to the IP address resolution provisions in the CTSA. The new and alternative paragraphs in the addendum have now been integrated into the code of practice.

Giving of data retention notices

Comments:

A number of responses welcomed the clarity this section provided to the processes underpinning the issuing of a data retention notice. The following minor suggestions were made:

- Making clear that the ICO will be notified if a CSP is retaining data under the Anti-Terrorism Crime and Security Act;
- Ensuring that the role of the ICO is discussed with a CSP ahead of a data retention notice being served;
- Setting out what steps would be taken if a new company entered a market where a notice had been issued to a category of providers; and
- Including more detail on what will be contained in a notice in respect of security of retained data.

Response:

Minor amendments were made to this section of the code to reflect these comments.

Comments:

Other suggestions included:

- Making clear that, where data is held by two companies, the question of who retains it should be considered on a case by case basis to avoid a single CSP being responsible for retention across multiple CSPs;
- Making clear that security of data should be considered by the Secretary of State when deciding to impose a data retention notice;
- Including specific factors that determine how long a CSP retains data for;
- Preventing a notice being served for certain data where a CSP considers that it cannot do something on technical grounds; and
- Including further guidance on how a CSP should notify the Home Office of new products and services.

Response:

Paragraph 3.15 of the code sets out the matters that must be taken into account when deciding whether to impose a data retention notice. Paragraph 3.17 makes clear that the Secretary of State will consider any other issue which is considered relevant to the decision. Home Office Ministers take their responsibilities when issuing a data retention notice very seriously, carefully

considering all relevant factors on a case by case basis. It would not be appropriate to list every possible issue which might be relevant in the code of practice. Where a CSP raises technological concerns the Home Office works with the CSP concerned to seek to identify a solution to the problem. The Home Office would not, however, serve a notice it knew a CSP could not comply with for technical reasons.

Further guidance on how a CSP under a data retention notice would notify the Home Office of new products and services will be issued to CSPs, but to ensure that the processes remain current it was not considered appropriate to include them in the code of practice.

Disclosure of data retention notices

Comments:

A number of respondents felt that data retention notices should be published.

Response:

As was the practice in respect of notices given under the 2009 Data Retention Regulations, the Home Office does not intend to publish the notices that are given to communications service providers. This is because to do so would risk undermining national security and the prevention and detection of crime, and for reasons of commercial confidentiality.

To provide a confirmation or denial as to whether a notice has been given to a specific communications service provider, or to disclose any details of such a notice, would allow interested parties to determine the extent and scope of work in this area. This would provide an insight into what the limit or scope of operational capability might be. Information concerning operational capability in respect of law enforcement and national security is highly sensitive information. It would be of significant value to criminal and terrorist groups. If, for example, the Home Office were to confirm that no notice had been given to a particular company, criminals and terrorists may choose to use that company rather than companies they know or suspect to be subject to a notice. The company without a notice would not retain data once they no longer had a business purpose for it, so whilst law enforcement agencies could request data from that provider, the data might well no longer exist in the absence of a retention obligation.

Similarly, if the Home Office were to disclose that notices are only given to telecommunications companies meeting certain criteria (for example a particular number of customers), criminals and terrorists would be in a position to divert their communications to services provided by other companies.

In addition, disclosure of the existence of a data retention notice given to a particular company would confirm the obligations placed on the provider by the Home Office. The commercial interests of that company would be prejudiced if significant numbers of customers transfer their business to companies who are not subject to a notice. There is genuine concern that financial and reputational harm would arise were such information to be made public.

Security of retained data

Comments:

A number of changes were suggested in this section:

- Amending references to security of data to cover security, integrity and destruction of data, where appropriate;
- Making clear that CSPs should comply with all reasonable requests from the Information Commissioner;
- Providing further detail on what data integrity means; and
- Making clear that CSPs can, with Home Office agreement, put in security controls or mitigations that differ from the code of practice where those alternative controls adequately protect the data.

Response:

Minor amendments were made to this section of the code to reflect these comments.

Comments:

One respondent suggested that security controls related to CSP disclosure systems should be covered in the acquisition and disclosure code of practice rather than the retention code of practice.

Response:

The Data Retention Regulations require CSPs to put in place technical and organisational measures to protect data against, among other things, unauthorised or unlawful access or disclosure. It is therefore right that this matter is covered in the retention code of practice which sets out how DRIPA and the Regulations made under it are implemented.

Comments:

Another respondent noted that it is not possible completely to eradicate security risks.

Response:

The data retention legislation and code of practice ensure that any risk is minimised by the CSP putting in the technical and operational controls with regard to the risks posed and the nature of the data being retained. The Information Commissioner audits the compliance of CSPs with these requirements. The Information Commissioner also has powers under data protection legislation to take action in the event of any inappropriate handling of data by communication service providers, or those who acquire it.

Comments:

Other issues that were raised were:

- Noting that some security guidance may be made publically available;
- Seeking clarity that internal CSP staff could undertake an IT Health Check, where suitably independent from those involved in data retention requirements;
- Seeking further guidance on security processes for CSPs; and
- Ensuring that issues where escalated to relevant oversight bodies.

Response:

These comments required no change to the code. The code does not preclude the use of internal staff to undertake an IT Health Check, or the publication of security guidance where appropriate. It already provides for the issuing of further guidance on security to CSPs involved in data retention and for the escalation of incidents to the relevant oversight body.

Use of retained data by CSPs

Comments:

The restrictions put in place on CSPs' use of data that was only retained because of the existence of a data retention notice were welcomed, but one respondent questioned whether it would ever be appropriate for a CSP to use retained data for marketing purposes

Response:

The code has been amended to make clear that the Home Office would not permit a CSP to use this data for marketing purposes.

Comments:

One respondent suggested that approval of any use of the data ought to be given by the Information Commissioner and not the Home Office.

Response:

The Information Commissioner's Office does not consider it appropriate that they approve such uses of the data, as it may conflict with its role in investigating any potential misuse of data by a communication service provider.

Comments:

One further respondent raised concerns about how a CSP may effectively ensure the security of data manage where shared systems are used for the retention of communications data.

Response:

The security requirements in the legislation and code of practice ensure that CSPs put in place adequate controls to protect against misuse of the data.

Comments relating to the acquisition code of practice

Comments:

Several respondents felt that all applications, or all applications regarding those in sensitive professions, should have judicial authorisation.

Response:

The system of internal authorisation, with the designated person, the guardian and gatekeeper role of the single point of contact (SPoC), and rigorous oversight provided by the Interception of Communications Commissioner, is a thorough, effective and efficient system. The Joint Committee on the Draft Communications Data Bill, who examined the system in significant detail, concluded it was the right system.

Comments:

One respondent argued that the applicant, single point of contact (SPoC) and designated person should never be the same individual.

Response:

The code that was consulted on had been strengthened to make it clear that this should be the case in all but exceptional circumstances. However, there are situations where it is prudent to allow an exception. For example, in situations of life and death and when a separate SPoC is not immediately available, the time taken to find a SPoC could lose crucial minutes, and thus the code allows certain exceptions.

Comments:

Another respondent felt that all safeguards and protections should be in primary legislation, rather than codes of practice.

Response:

The purpose of the code of practice includes providing guidance and information relating to the rigorous safeguards that are already contained in the primary legislation itself. Section 72 of RIPA requires that a person exercising any power or duty covered by a code of practice has regard to the applicable provisions of that code, and the provisions of the code may be taken into account by a court, the Interception of Communications Commissioner or the Information Commissioner.

Comments:

A small number of respondents felt the duties and requirements of CSPs should be made clearer, including on what checks a CSP should make on the application.

Response:

The code already contains information that sets out the duties of the CSP when receiving a notice and explains that a CSP may be provided with details of an authorisation. Where a notice or authorisation is authorised, it is the legal duty of the CSP to ensure the data is disclosed as long as it is reasonably practicable for the CSP to do so. Only accredited SPoCs may use a CSP's secure auditable communications data acquisition system, and only with authorisation by an appropriate designated person.

Comments:

A number of respondents believed that the communications data of journalists and others in sensitive professions, particularly lawyers or Members of Parliament, was itself subject to professional or legal privilege.

Response:

The Interception of Communications Commissioner, in his report of 4 February 2015 on the acquisition of communications data of journalists by police, is clear that this data is not privileged: "the communications data retained by CSPs do not contain any material that may be said to be of professional or legal privilege – the fact that a communication took place does not provide what was discussed or considered or advised." (paragraph 6.16). The Government agrees with the Commissioner's position.

There are, however, particular issues regarding the sensitivity of this communications data, which is why the code that underwent public consultation included a new subsection on those who are members of professions who handle privileged or otherwise confidential information. This part of the code and a number of other parts of the code have been further enhanced following the responses to the consultation, and the report of the Commissioner. This includes that all such applications must be flagged to the Commissioner at the next inspection.

Comments:

In related responses, some respondents felt that the list of professions given to exemplify those that handle privileged or otherwise confidential information should be expanded beyond the current list of medical doctor, lawyer, journalist, Member of Parliament, and minister of religion. Others felt that further guidance was needed on what should be recorded by public authorities.

Response:

While the list that is given corresponds to that provided in other related codes of practice, it is not an exclusive list and we are working with the College of Policing to enhance training so that law enforcement are fully aware of this. The section on record keeping has also been clarified in the amended code and the Interception of Communications Commissioner's Office intends to publish specific guidance on the enhanced record keeping.

Comments:

A small number of comments were made on the section regarding the public emergency call service (999/112 calls). One respondent questioned if the emergency period following a call, during which the emergency service can call upon an emergency operator or CSP to disclose data about the maker of any emergency call would remain one hour.

Response:

The Government is clear that one hour is an appropriate time frame (the so-called 'golden hour') and there are no current plans to increase or reduce the time available.

Comments:

A number of comments were made on the keeping of records.

Response:

The Government is committed to increased transparency. The section on the keeping on records is significantly expanded: the 2007 code, for example, listed only four specific items of data that should be recorded by each relevant public authority and the new code lists twenty. IOCCO intends to publish guidance on the specifics of what they require for each item of data that is listed in the code. This will be available from their website.

Comments:

More clarity was sought in the code regarding CSPs' duties under the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the privacy regulations").

Response:

While duties under the privacy regulations are not governed by the acquisition code, a small number of changes have been made to clarify the situation, including the addition of a footnote to the effect that the requirements of the acquisition code do not affect a CSP's statutory duties under the privacy regulations.

Comments:

A small number of respondents asked whether public authorities should retain excess data.

Response:

The code is clear that, for criminal investigations, there is a requirement to record and retain relevant data, even if that data was disclosed or acquired beyond the scope of a valid notice or authorisation. This requirement would apply in law even if it were not stated in this code.

Comments:

Greater clarity was sought on data protection principles, particularly on the duties of public authorities relating to communications data they have acquired.

Response:

Data acquired by public authorities is governed by the Data Protection Act 1998 and the code is clear that this is the case. The code has been amended to add further information, for example providing additional links to resources available from the Information Commissioner's website.

Comments:

It was considered by some respondents that processes under the Mutual Legal Assistance treaty (MLAT) should be used to acquire data from CSPs based outside the UK.

Response:

MLAT requests are appropriate when communications data may be required for use as evidence. However, mutual legal assistance conventions and agreements are not an adequate alternative to direct cooperation on communications data requests made under RIPA. The several months MLAT requests can take mean it cannot cope with the speed and volume of communications data requests necessary to conduct effective investigations. Nonetheless, we continue to look at MLAT processes and procedures to see where efficiencies can be made.

More fundamentally, MLAT requests do not address the broader capability gaps we face in relation to retention. If certain data types are not generated collected and retained they will never be available via this process. Sir Nigel Sheinwald has been appointed to lead discussions with the US Government, key international partners and CSPs, to assess and develop formal arrangements for the accessing of data for law enforcement and intelligence purposes held in different jurisdictions.

Comments:

One correspondent commented that the only circumstance in which the Interception of Communications Commissioner shall notify an individual of acquisition or disclosure of data relating to them is where the individual "has been adversely affected by any wilful or reckless failure by any person within a relevant public authority" and that this is a high bar.

Response:

It would not be appropriate to tip-off an individual that an investigation is on-going. It is open to anyone to complain to the independent Investigatory Powers Tribunal if they feel the powers in RIPA have been used unlawfully against them.

Comments relating to the communications data of journalists

Comments:

The significant majority of responses to the consultation were concerned wholly or in part with communications data relating to journalists or their sources. Over two hundred of the responses received were based on a response template created by the National Union of Journalists (NUJ). These responses requested four changes to the process for such data:

- An independent and judicial process
- Automatic and mandatory prior notification of requests
- Mechanisms to challenge an application and the right of appeal
- New primary legislation to replace the existing powers and offer a "shield law" for journalists

These changes were also requested separately and together by a number of other respondents, including a number who provided examples of British and European case law.

Response:

The independent Interception of Communications Commissioner (IOCC) carried out an inquiry into the issue of police acquisition of the communications data of journalists. He published a report on his inquiry on 4 February 2015, which included a significant examination of the case law.

The IOCC report (available from his website) is clear there was no systematic abuse. Specifically, “forces are not randomly trawling communications data relating to journalists in order to identify their sources” (IOCC emphasis, paragraph 8.3). Rather, the applications primarily “related to investigations where public officials were suspected of criminal conduct or where a media organisation had voluntarily disclosed information to the police relating to what they believed to be criminal conduct for investigation”.

IOCC is also clear that RIPA was not used to undermine the Police and Criminal Evidence Act 1984 (PACE) or other legislation. He makes clear that RIPA is the only appropriate legislation for the police and other public authorities to use to acquire communications data and the use of RIPA does not circumvent any other legislation, including any requirements for prior notification of applications (paragraphs 6.10-6.15).

Nonetheless, IOCC found that, in a number of applications, the processes set out in RIPA were not sufficiently well followed, particularly with regard to consideration of the right to freedom of expression. He also found that there was not sufficient detail in the code of practice on what was required in such considerations. He therefore made two recommendations (paragraph 8.9):

> *1. Judicial authorisation must be obtained in cases where communications data is sought to determine the source of journalistic information.*
>
> *2. Where communications data is sought that does not relate to an investigation to determine the source of journalistic information (for example where the journalist is a victim of crime or is suspected of committing a crime unrelated to their occupation) Chapter 2 of Part 1 of the Act may be used so long as the designated person gives adequate consideration to the necessity, proportionality, collateral intrusion, including the possible unintended consequence of the conduct. The revised Code contains very little guidance concerning what these considerations should be and that absence needs to be addressed.*

The Government immediately accepted both of these recommendations. The Government has been clear that a free press is fundamental to a free society and nothing should be done which might endanger it.

In response to the first recommendation of IOCC and addressing comments proposing judicial authorisation, and as a stop-gap until legislation can be enacted in the next Parliament, the acquisition code will now require applications to determine the source of journalistic information to be processed under PACE, and equivalent legislation in Northern Ireland and Scotland. The PACE process requires judicial authorisation.

To show its intent and its commitment to protect and preserve the freedoms that journalists in the UK enjoy, the Government brought forward an amendment during the passage of the Serious Crime Act that requires the acquisition code to reflect any IOCC report and for the Government to consult with IOCC on the code. The Government also published a draft clause that gives full effect to the Commissioner's recommendation, to be included in future legislation. Legislation will be needed early in the next Parliament, following the review by David Anderson QC and before the December 2016 sunset of DRIPA.

In response to the second recommendation and those respondents who felt the code was not clear enough on necessity, proportionality, freedom of expression, and collateral intrusion, the code now contains:

- Clarification throughout the code that the right to privacy is not the only right that must be taken into account when making or considering applications and that, in particular, the right to freedom of expression must also be considered where relevant;
- New, additional guidance on necessity and proportionality to aid those writing and considering applications for communications data, with detail on collateral intrusion and unintended consequences;
- A significant increase in the detail provided on those in professions that handle privileged or otherwise confidential information, including detail on considerations of the public interest and laying out the requirement for law enforcement to use PACE for applications to determine journalistic sources; and
- A requirement for authorities to flag to IOCC, at the next inspection, all applications for communications data relating to those on in professions that handle privileged or otherwise confidential information.

It remains the case that anyone, including a journalist, can report any application for communications data made under RIPA to the Investigatory Powers Tribunal, an independent tribunal made up of senior members of the judiciary and the legal profession. The Tribunal has full powers to investigate and decide any case within its jurisdiction which includes the acquisition and disclosure of communications data under RIPA. Contact details for the Tribunal are listed in the acquisition code.

The code does not contain a requirement to flag applications for the communications data of journalists, or others in sensitive professions, to those to whom the data relates. This was not something that was recommended by the Commissioner. It has also never been the practice in this country that those whose communications data is obtained are notified. There are obvious reasons for this, given that serious or organised crime may be under active investigation. We do not propose to depart from that policy.

Comments:

A number of respondents felt that the records kept by authorities and CSPs, or those published by IOCC in his annual report, were not broad enough to identify applications relating to journalists. It was also felt that there should be greater oversight by IOCC of such applications.

Response:

The language on the new reporting requirements has been clarified so that, when an application has been made for communications data relating to a member of a profession that handles privileged or otherwise confidential material, including journalists, the specific profession is recorded. As noted above, the Interception of Communications Commissioner's Office (IOCCO) will be issuing additional guidance on the enhanced record keeping of the new code.

Oversight of all applications for communications data is provided by the IOCC, who is a retired judge. He and the members of IOCCO inspect all public authorities with access to communications data, investigate all errors and he must (following DRIPA) provide a report to the Prime Minister every six months. The code now requires that applications for data of those in such professions must be flagged to the Commissioner at the next inspection.

Comments:

A number of respondents raised concerns about whether the records kept will be sufficient to identify when data has been acquired regarding a 'whistleblower'.

Response:

Under RIPA, police and other public authorities cannot acquire communications data unless it is for one of the listed statutory purposes. These purposes do not include the acquisition of data regarding whistleblowers where no crime has been committed nor the acquisition of data for political or reputational reasons. Further, if a crime has been committed, it is the duty of the police to investigate.

However, as noted above, IOCC did establish that a number of the applications they considered did not sufficiently record the consideration of necessity and proportionality in the application, nor was there sufficient guidance in the code regarding these considerations. We have fully accepted his recommendations and have made the changes to the code listed above in response to his recommendations and the comments received in this consultation. In addition to these changes to the code, we are already working with the College of Policing to amend training on communications data for the police and law enforcement, to improve both the knowledge of those involved in the process and the quality of applications.

Comments:

A number of respondents commented on the terminology used. This included those who asked who should be considered a journalist, particularly in the age of the internet, and what was meant by the special consideration required when making applications for communications data relating to a person who is a member of certain professions.

Response:

The enhanced training described above will take into account these comments to ensure that applicants, SPoCs and designated persons are aware of their responsibilities regarding such applications under the new code.

In particular, regarding 'who is a journalist', the training will reference Annex D of the IOCC report: "Proposed Guidance for Officers Considering a Request for a Journalist's Communications Data under RIPA 2000" by Professor Anne Flanagan, Professor of Law at the Centre for Commercial Law Studies of Queen Mary University of London.

Comments:

Some respondents considered that data relating to those in sensitive professions should not be retained or that specific reference should be included in the retention code of practice to consideration of excluding certain groups from retention obligations.

Response:

It is impossible to predict in advance who may be involved in criminality or be a victim of crime. Were data not retained in relation to journalists, for example, the police may be unable to effectively investigate any crime which they commit or are victim of. An amendment has been made to the retention code of practice to make clear that data retained cannot be accessed by public authorities without consideration of the impact on a person's privacy and, where relevant, freedom of expression.