Home Office

Investigatory Powers (Amendment) Act 2024

Response to consultation: Codes of Practice and Notices Regulations

March 2025

Contents

Background

Investigatory Powers (Amendment) Act 2024

The Investigatory Powers (Amendment) Act 2024 (the 2024 Act) received Royal Assent in April 2024. The 2024 Act made targeted changes to the Investigatory Powers Act 2016 (IPA) to enable law enforcement and intelligence agencies to continue to tackle a range of evolving threats in the face of new technologies and increasingly sophisticated terrorist and criminal groups.

Much of the operational detail on the use of powers provided for in the IPA is necessarily set out in guidance, rather than on the face of the primary legislation. This is delivered through statutory Codes of Practice (the Codes), which provide information on the processes associated with making an application to use, and using, each of the powers, as well as the safeguards and oversight arrangements that will ensure the powers are used in the intended manner and protect fundamental human rights. The Codes have statutory force and individuals exercising functions to which the Codes relate must have regard to them.

Several of the changes made by the 2024 Act relate to the Notices regime, with the aim of helping the UK anticipate and develop mitigations against the risk to public safety posed by multinational companies rolling out technology that precludes lawful access to data for the statutory purposes set out under the IPA. One such change is the introduction of Notification Notices, which, when given by the Secretary of State to a relevant operator, has the effect of requiring that operator to notify any proposals to make relevant changes to systems or services specified in the Notice. The 2024 Act introduced a delegated power for the Secretary of State to set out in Regulations further details regarding relevant changes and associated thresholds that may trigger the Secretary of State to issue a Notification Notice to an operator.

Consultation

On 14 October 2024, the Home Office launched a 12-week public consultation to seek views on eight Codes and one set of draft Regulations.

These include five updated Codes on Bulk Personal Datasets, Communications Data, Bulk Communications Data, Equipment Interference, and Interception. They also include new Codes on Bulk Personal Datasets with a low or no expectation of privacy and third party Bulk Personal Datasets, which relate to regimes brought about by the 2024 Act, as well as a new Notices Code, which brings together existing guidance and new text covering amendments made by the 2024 Act into a single Code.

The Regulations covered within this consultation (published in draft as *The Investigatory Powers (Notification Notices, Review Periods and Technical Advisory Board) Regulations*) amend the existing *Investigatory Powers (Review of Notices and Technical Advisory Board) Regulations 2018* to reflect the changes made to the Notices regime by the 2024 Act and provide further legislative detail on the new Notification Notices.

Input provided by operational partners, Telecommunications Operators and parliamentarians during the passage of the 2024 Act was taken into consideration when preparing the Codes and the Regulations, ahead of the consultation, and this feedback was reflected in the published drafts where appropriate.

Responses

We received a total of 19 responses to the consultation. Responses came from a range of stakeholders, including interest groups, charities, public authorities, think tanks, technology companies, trade associations and members of the public.

While most respondents did not specify whether they were content for comments to be attributed to them, some respondents requested that their details not be disclosed. For consistency, we have chosen not to attribute any comments to specified individuals or organisations.

Table of respondents

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

Nature of response	Number of respondents
Interest groups and charities	4
Public authorities	3
Think tanks	3
Trade associations	3
Technology companies	2
Other bodies	1
Other members of the public	3

Consultation responses and government response

Responses to the consultation primarily focused on the Codes relating to the Notices regime, Communications Data, and Bulk Personal Datasets with a low or no expectation of privacy. There were only limited references to the draft Codes relating to Equipment Interference or Interception of Communications.

The responses included various suggestions for amendments to the draft Codes and Regulations. We have made several changes as a result, which are outlined below. These include stylistic changes, further clarity on processes, and changes to the Technology Advisory Board's membership requirement.

The consultation sought views specifically on the draft Codes and Regulations, rather than the provisions included within the 2024 Act itself. The Codes and Regulations cannot include provisions which contradict those within the primary legislation, so while some respondents have suggested amendments to the 2024 Act, these have not been acted upon.

Bulk Personal Datasets: Low or no expectation of privacy (Part 7A)

Theme 1: Types of dataset within scope of the regime

We received several comments requesting that the Code makes clear that certain categories of datasets are out of scope of Part 7A. Concerns were mainly centred on medical records, social media data and hacked or leaked datasets.

Response

The question of whether a dataset meets the low or no reasonable expectation of privacy test will be assessed on a case-by-case basis, having regard to all the circumstances, including the factors set out in the 2024 Act. An expectation-based test must be applied to determine whether the nature of the bulk personal dataset is such that individuals to whom the personal data relates could have no, or only a low, expectation of privacy in relation to the data. This is a nuanced assessment which is based on the individual qualities of a given dataset, so creating a list of datasets that are out of scope of Part 7A would place unnecessary and arbitrary restrictions on the regime.

Part 7A should not be used for datasets containing information of particular sensitivity. This means that where the nature of the information in a dataset is likely to give rise to a greater intrusion from its retention and examination, the Part 7 regime should be used. This will ensure that the rights of the individuals to whom the

data relates are adequately protected whilst also enabling the intelligence services to make more effective use of bulk datasets.

Theme 2: The reasonable expectation of privacy test and factors

We received concerns regarding the reasonable expectation of privacy test, and the application of the factors, including the suggestion of including further hypothetical dataset examples against each description of the factors. These were focused on the extent to which data has been made public, the extent to which the data has already been used in the public domain, and the use to which the data will be put.

Response

The factors in section 226A of the IPA, for which the Code provides further detail, were chosen because they are most relevant to the context in which the reasonable expectation of privacy test will be applied and have been drawn from existing case law. They provide a guide for the decision-maker in reaching a conclusion as to the nature of the dataset. We believe that the existing description of the factors within the Code provides a strong and clear demonstration of how the test is to be applied and relevant considerations for decision-makers to have regard to.

Theme 3: Machine Learning and capability development

We received comments regarding the use of datasets for Machine Learning and capability development purposes. This included comments seeking clarity as to whether personal data in a Part 7A dataset could be used to train Machine Learning models. There were also concerns regarding whether the data used to train Machine Learning or AI models correctly meets the low/no test.

Response

The Part 7A regime is about ensuring that data that is assessed to have a low or no reasonable expectation of privacy has appropriate and proportionate safeguards when retained or used by the intelligence services. The Code states that the use to which data will be put will form part of the relevant circumstances which inform the assessment of the reasonable expectation of privacy of that data, which could include capability development. Paragraph 4.26 of the Code already sets out that where an intelligence service assesses that the use of the data is a relevant factor in determining the reasonable expectation of privacy, then this should be justified when it is under consideration for authorisation.

Theme 4: The concept of low/no reasonable expectation of privacy and the regime's foreseeability and accessibility

We received responses which set out concerns about the low/no reasonable expectation of privacy test and its foreseeability and accessibility. Some respondents requested that we revisit the test and apply further safeguards, or that the Codes be clearer with the criteria and proportional thresholds for determining when a dataset would qualify as having low/no reasonable expectation of privacy.

Response

The question of whether a dataset meets the low/no reasonable expectation of privacy test will be assessed on a case-by-case basis, including the factors set out in the 2024 Act. The Code makes clear that the test for considering a dataset as low/no expectation of privacy is framed around the concept of 'reasonable expectation of privacy'. This is the jurisprudential touchstone for the engagement of Article 8 of the European Convention on Human Rights. The Code also sets out several factors to be considered when assessing the expectation of privacy of a dataset. These factors are drawn from existing case law and drafted so that there is flexibility to accommodate future developments.

In addition to the factors set out in section 226A(3) of the IPA, and expanded on in the Code, the Code imposes the further requirement that an application for an authorisation must explain why it is considered that the test in section 226A applies, the operational and legal justification, as well as the necessity and proportionality of the proposed retention and/or examination of the dataset.

Theme 5: Part 7A datasets containing a small amount of data in respect of which there is more than a low reasonable expectation of privacy

We received comments seeking clarity regarding Part 7A datasets containing a small amount of data where there is more than a low reasonable expectation of privacy. This included seeking assurances as to what is meant by a small amount and the way in which this is managed.

Response

The Code outlines that a bulk personal dataset which does not meet the test set out in section 226A(1) cannot be authorised as a low/no dataset. It also sets out that an application to authorise retention of a dataset under Part 7A should include an explanation of the necessity, and the proposed safeguards with its retention and examination. This also applies where the presence of a small amount of data which is considered to have more than a low reasonable expectation of privacy is suspected, but where an exhaustive examination is not feasible, such as where a dataset is very large.

The section 226D safeguard and associated explanation in the Code outlines a clear process for ensuring information is handled appropriately where information of a particular sensitivity is subsequently discovered within a dataset. Robust independent oversight of the Part 7A regime will be provided by the Investigatory Powers Commissioner, who will audit and inspect the intelligence services' compliance with the legislation and adherence to the Code.

Intelligence services' use of third party bulk personal datasets (3PDs) (Part 7B)

Theme 1: Legality of third party datasets

We received several comments regarding the legality of the datasets which the intelligence services will be examining under the 3PD regime. Concerns centred around whether the data gathered by third parties has been obtained and handled lawfully, including in line with human rights and data protection laws.

Response

The Code outlines that intelligence agencies' access to 3PDs is subject to safeguards, including double-locked warrants which are issued by the Secretary of State, having been approved a Judicial Commissioner. Intelligence agencies can only examine a 3PD when it is necessary and proportionate, and in accordance with relevant legislation such as the Data Protection Act 2018, the Intelligence Services Act 1994, or the Security Service Act 1989. Any examination of a 3PD would be undertaken in accordance with the requirements of section 226IA of the IPA and the 3PD Code of Practice. In addition to the safeguards applying to intelligence agencies, the third parties themselves also have legal obligations, as they are data controllers and are responsible for ensuring data processing is compliant with data protection legislation.

Theme 2: Granting intelligence agencies consent to access 3PDs

Some responses suggested that the Code of Practice be clear in outlining that third parties are not obliged to give intelligence agencies access to datasets if they do not want to, as the third parties are the ultimate owners and controllers of the datasets.

Response

In order to examine 3PDs intelligence agencies must obtain "relevant access", which must be directly arranged with the third party to have electronic access to the data. The Code of Practice provides detail under "*Initial Inspection*", which clarifies that

intelligence agencies should work with third parties on the practical steps to establish if access is suitable and how it can be provided. The Investigatory Powers Commissioner has responsibility for overseeing the 3PD regime and can seek to inspect how an intelligence service is applying the initial inspection provisions with the third party.

Theme 3: Safeguards

Responses questioned how robust the safeguards are for 3PDs, including around sensitive data and handling conditions. One response touched on the fairness of the warranty process and the Secretary of State issuing warrants, while another queried the clarity of the definition of “generally available” datasets within the 3PD context.

Response

The safeguards outlined in the Code of Practice have mirrored, where possible, the existing and well-established safeguards that underpin the most intrusive powers in the IPA. The double lock provides extra assurance that 3PD warrants will only be issued when it is necessary and proportionate, having been independently assessed by a Judicial Commissioner. The Code of Practice has provided detail of these scenarios and the language used is intended to be futureproof and agile as datasets develop.

The datasets to which intelligence agencies are granted access may be ‘live’ and therefore continually updated by third parties. This is likely to happen constantly as part of normal business, without the intelligence service being informed it is taking place. If, when the dataset is examined, it becomes apparent that sensitive data is present, additional handling instructions outlined in the Code are applicable.

The Code provides further detail on what is in scope of the “generally available” definition. Due to the varying types of datasets and third parties, the definition is required to cover a range of scenarios.

Theme 4: Retention of 3PDs

Some responses sought clarity on the process for when intelligence agencies would be able to retain 3PDs on their own systems.

Response

The Code of Practice already confirms that should the intelligence service wish to retain data that itself constitutes a bulk personal dataset, they would need to apply for a warrant under Part 7 or Part 7A IPA as appropriate.

Intelligence services' use and retention of bulk personal datasets (Part 7)

We received limited responses specifically on the Part 7 Code, although those that we did receive outlined a number of concerns with various aspects of the regime, including the very concept of bulk personal datasets, necessity and proportionality, protected data, safeguards, the warrantry process, retention and deletion of data, and errors.

The Government is of the view that the Part 7 Code provides detailed statutory guidance to which practitioners must have regard and provides sufficient foreseeability as to the operation of the power. The concept of bulk personal datasets goes beyond the scope of this consultation, although it is worth noting that the regime has been tested in the courts, and the Court of Appeal has found that both the regime itself and the existing statutory Code of Practice provide "clear and detailed rules"[1].

Communications Data

Many of the responses to the draft Communications Data (CD) Code of Practice were positive and supportive of the changes made to the CD regime in the 2024 Act, and the additional clarity provided by the updated Code. In particular, respondents welcomed the changes to section 11 of the IPA, finding the list of examples of what will amount to 'lawful authority' and clarity on the lawfulness of sharing of CD between public authorities 'wholly or mainly' funded by public funds to be helpful additions. Several of the responses proposed stylistic and formatting changes to the Code, many of which have been taken on board.

Theme 1: Definitions

While some respondents found the definitions provided in the CD Code of Practice an improvement on the previous Code, others considered that the definitions of 'Communications Data' and 'Telecommunications Operator' are either too broadly or too narrowly defined. Some responses queried whether an IPA Part 3 authorisation applies to companies whose 'parent' companies are based outside of the UK. One response raised concerns that the 'serious crime' definition, as defined in the primary legislation, is inconsistent with other pieces of legislation, and risks CD being unlawfully disclosed.

<u>Response</u>

[1] Paragraph 214 of Liberty v SSHD and Ors. [2023] EWCA Civ 926.

The broad services offered by Telecommunications Operators and the specific nature of investigations means that it would be more suitable to provide further support on the definitions of 'Communications Data' and 'Telecommunications Operator' on a case-by-case basis, rather than through revisions to the Code itself. The Home Office already works closely with the CD user community on the changes brought about by the 2024 Act and will continue to offer support as required.

Regarding queries about the impact of an IPA Part 3 authorisation on companies with parent companies outside the UK, such authorisations have extra-territorial effect, and as such can compel the acquisition of CD from Telecommunications Operators as defined by the IPA (section 85). The CD regime has robust safeguards in place, with all applications from public authorities undergoing IPCO's independent scrutiny through prior authorisation and/or through the post-hoc inspection process. This independent oversight is effective in identifying any risks of unlawful acquisition or disclosure. The definition of 'serious' crime in the legislation and its consistency with other pieces of legislation was not within the scope of this consultation.

Theme 2: Compliance obligations placed on Telecommunications Operators

Some respondents requested additional clarity on the processes and timelines in respect of error reporting to the Information Commissioners Office (ICO) and the Investigatory Powers Commissioners Office (IPCO). One response raised concerns about introducing additional regulatory requirements on what they considered to be 'newly defined' Telecommunications Operators and their ability to meet their obligations with regulators in respect of error reporting, data retention and disclosure notifications.

Response

In consultation with the ICO and IPCO, and considering the feedback received through this consultation, the Home Office has updated the section of the CD Code on error reporting (Chapter 15) to introduce further clarity on process, timelines and error reporting obligations in CD acquisition and disclosure.

Neither the 2024 Act, nor the draft CD Code of Practice, expand the definition of a 'Telecommunications Operator'. Rather, the Act and the Code have sought to provide further clarity through express drafting and examples of the types of services and organisations that meet the definition of a 'Telecommunications Operator'. The IPA's definition of a 'Telecommunications Operator' does not have any direct bearing on the wider regulatory frameworks for the telecommunications sector, such as with Ofcom licensing.

Notices

Following the responses received, a number of changes, documented below, have been made to the Notices Code of Practice, to provide additional clarification and consistency where required. The draft Regulations will also be amended in relation to the minimum level of membership to the Technical Advisory Board.

Theme 1: Terminology

A number of respondents raised concerns that terminology used in the draft Regulations is inadequately defined, which may result in uncertainty or terms being overly broad in application. This includes the terms “relevant change” and “reasonable time”, in relation to Notification Notices.

Response

Prior to any Notice being issued, a consultation process will be undertaken between the Government and the operator, where the scope of the Notice and other specifics will be discussed in depth. “Relevant change” and “reasonable time”, which relate specifically to Notification Notices, have been kept deliberately broad. This is because the companies a Notification Notice could be given to vary greatly, and therefore what constitutes a “relevant change” does as well. For this reason, the Code provides examples of what may be considered as “relevant changes” and clarifies that what will amount to a “reasonable time” will vary depending on the exact change, since it is a proportionate test. Further discussions on expectations can be held during the consultation period with the individual company, with guidance and advice being made available to companies both during their individual consultation periods and once a Notification Notice is issued.

Theme 2: Technical Capability Notice (TCN) Review Process

Some respondents sought further clarity on the new processes for the review of TCNs.

Response

Following the issuance of a Notice (except a Notification Notice), if an operator is dissatisfied with the relevant terms, they have the statutory right to refer the Notice – or part of it – back to the Secretary of State for review. The 2024 Act included a regulation-making power, which allows the Secretary of State to specify in Regulations the time limit within which a Notice review must be completed. Those draft Regulations were included in this consultation.

The draft Regulations set out that the overall length of time the review of a Notice can take is 180 days (the “review period”). The review period can be extended at the

request of the operator, the Judicial Commissioner, or the Secretary of State; all three parties must agree to any extensions.

When a Notice is referred for review, the Secretary of State must consult the Technical Advisory Board (the TAB), which considers the technical requirements and financial consequences of the Notice. An independent Judicial Commissioner will consider the proportionality of the Notice. The Secretary of State and the operator have the opportunity to provide evidence and make representations to the TAB and Judicial Commissioner. Following consideration, both the TAB and the Judicial Commissioner must report their conclusions to the operator and the Secretary of State. Based on this, the Secretary of State must decide whether to confirm the effect of the Notice, vary the Notice, or revoke the Notice. The decision is then reviewed and approved by the Investigatory Powers Commissioner. The draft Regulations stipulate that the Secretary of State has 30 days to reach this decision (the "relevant period"). This period can only be extended by the Secretary of State in exceptional circumstances, as laid out in the Regulations, and this extension cannot take the review period beyond 180 days.

Following changes made by the 2024 Act, whilst a TCN is under review, the operator must not make any changes during the review period that would negatively impact lawful access. Operators will not be required to make changes to comply specifically with the Notice. However, they will be required to maintain the status quo, meaning that if lawful access was available before the Notice was given, then it must be maintained during the review period. This will be without prejudice to the outcome of the review.

A clear timeline is of benefit to all parties involved and it provides operators the certainty they require regarding the length of time the review can last, and therefore how long the status quo will need to be maintained.

Theme 3: Impact on Innovation

A number of respondents raised concerns that Notification Notices would inhibit the ability of technology companies to innovate or make necessary security updates to their products. This concern was repeated in relation to the need for operators subject to a TCN to maintain the status quo during any review of that Notice.

Response

Several responses went beyond the scope of the Code of Practice and Regulations, and have been addressed previously[2].

[2] House of Lords, Hansard vol. 824 no. 7 col. 652-653, 20 November 2023

However, it is worth reiterating that, as noted during the passage of the 2024 Act, a Notification Notice does not give the Secretary of State any powers to intervene in or veto the rollout of a product or a service, and the Code of Practice makes explicit that security patches cannot be within the scope of a "relevant change" [3]. The notification requirement created by a Notification Notice is intended to ensure that there is time for appropriate consideration of the operational impact and relevant mitigations. This does not represent a novel or significant change to the existing Notices regime, which has operated for decades without a demonstrable impact on innovation.

Some responses touched on the interaction between Notification Notices and the pre-existing Notices regime. The process for issuing Notification Notices is entirely separate to the issuing of any other Notice, and the existence of a Notification Notice does not predetermine the use of another type of Notice. If the Secretary of State were to consider giving a TCN to an operator subject to a Notification Notice, a new consultation would need to be initiated, separate to any consultation on the Notification Notice. The existence of a Notification Notice does not, on its own, expedite the TCN process or automatically result in the subsequent giving of a Notice.

Theme 4: Technical Advisory Board (TAB) Membership

A concern was expressed that lowering the minimum level of TAB membership from thirteen to seven members would undermine the resilience and flexibility of the Board, and risk leaving the TAB without sufficient capacity to manage its workload. Additionally, a concern was raised that the corresponding reduction in the minimum numbers of industry and Government representatives may result in a reduced diversity of perspectives.

Response

We recognise these concerns and have made amendments to the Regulations to retain the current minimum membership requirement of thirteen TAB members, including retaining the minimum membership requirement of six representatives from both industry and Government.

Theme 5: Notification Notice Procedure

Respondents raised queries around the issuing and implementation of Notification Notices. There was concern about the limited amount of guidance on the

[3] House of Commons, Public Bill Committee Official Report col. 55, Investigatory Powers (Amendment) Bill, 07 March 2024

consultation with operators preceding the issuing of a Notice, including the format and timeline of that consultation, and the uncertainty this might create for companies.

Respondents queried how the requirement for non-disclosure of a Notice would function in practice, seeking clarity regarding the circumstances in which they must seek the Secretary of State's permission to disclose the existence of the Notice within their organisations.

Respondents also sought clarity on when a Notification Notice, once issued, would come into effect. There were concerns that without a "grace period", operators would have insufficient time to establish compliance procedures.

Response

In advance of issuing a company with a Notification Notice, the Government will consult with that company on the content and practicalities of the Notice. The format of this consultation will be necessarily adapted to suit the individual company, taking into account factors like the structure and size of the Telecommunications Operator and the services it provides.

Further guidance and advice will be made available to companies both during the consultation process and once a Notification Notice has come into effect. This will provide clarity on implementation, including relevant security and disclosure considerations. These considerations will also be discussed during the consultation period itself, to ensure the procedures around the Notice are understood, suitable for each individual company and that a pragmatic approach to implementation is undertaken. Therefore, we do not consider it helpful to be overly prescriptive in the Codes themselves on this topic.

The concerns raised about timing for the coming into effect of Notification Notices are recognised. The Code of Practice references that the point at which a Notice comes into force can be specified in the Notice. A pragmatic approach to the implementation of Notification Notices, including the date on which Notices come into effect having been given, will always be prioritised. It is anticipated that the collaborative consultation process will inform these considerations and sufficient time will be afforded to enable preparatory steps to be taken where necessary.

Theme 6: Conflicts of Law

Some respondents have raised the topic of conflicts of law. They note that the Code of Practice contains a high-level approach to address these, but express concerns that the language is insufficiently detailed.

Response

The Government has a long history of working with companies when issues regarding conflict of law arise. By their nature, conflicts of law are case-by-case issues and cannot be addressed in a blanket fashion. It is appropriate to keep language in the Code of Practice high-level to allow for this flexibility.

Interception of Communications

Only one comment was received regarding the Interception of Communications Code of Practice, which suggested further guidance for overseas Telecommunications Operators regarding the modification of targeted interception warrants. The Code of Practice already provides detailed guidance on the modification of these warrants, and we consider that any additional support or guidance would most appropriately be provided on a case-by-case basis.

Equipment Interference

The limited responses received regarding the Equipment Interference Code of Practice sought further clarification on the duty of a Telecommunications Operator to assist with equipment interference warrants. In response, we have made minor amendments to Chapter 7 of the Code to provide greater clarity on these duties.

Next steps

A single set of Regulations will be laid before Parliament. This will include the provisions outlined in the draft Notices Regulations, as well as some additional provisions to bring the new and updated Codes into force. The Regulations will go through the affirmative procedure, meaning a debate and vote in each of the Houses of Parliament is required before they can be made and come into effect. The updated Codes and an Explanatory Memorandum will be published alongside the Regulations when they are laid in Parliament.