January 6th, 2025

The Home Office
UK Government

Written Evidence Submission on the Investigatory Powers (Amendment) Act 2024 Regulations and Codes of Practice

The Center for Data Innovation appreciates the opportunity to submit written evidence in response to the Home Office call for submissions to its first consultation on the Investigatory Powers (Amendment) Act 2024 (IPA 2024) Regulations and Codes of Practice.

The Center for Data Innovation studies the intersection of data, technology, and public policy. Its mission is to formulate and promote pragmatic public policies designed to maximise the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

EXECUTIVE SUMMARY

The IPA 2024 came into law on 25th April 2024, amending several provisions within the pre-existing Investigatory Powers Act 2016 (IPA 2016) which addressed the interception of communications, acquisition of bulk personal datasets (BPDs), and retention and evaluation of information related to investigatory powers and national security. The Secretary of State, as required by the new law, drafted regulations and new codes of practice to govern the use of powers afforded by the IPA 2024 to public authorities, including police and intelligence services. Eight new or revised codes of practice have been put forward for consultation. We offer six key recommendations, split across the different annexes of the codes:

The Secretary of State should amend Annex A relating to BPDs with a low or no expectation of privacy (LNEP) to:

1. Clarify the application of the factors listed in section 226A(3) IPA 2024 with stronger hypothetical examples in the code.
2. Set clear criteria and proportional thresholds for determining when a dataset qualifies as LNEP.

Annex H relating to the Notices Regime should be amended to:

1. Limit the scope of Notification Notices to “relevant changes” that demonstrably and significantly impact lawful access capabilities under the legislation, supported by a body of tangible evidence.

2. Limit the scope of "negative effect" for the review process for data retention, technical capability, and national security notices.
3. Expand guidance on the decommissioning of services, in particular confirming that the UK government will not unreasonably impede any decommissioning of a service falling within the notice regime.

Recommendations of general application to the codes:

1. Ensure the section 2(2) IPA 2016 considerations are afforded the appropriate level of scrutiny by public authorities and that these authorities consider all factors when executing their duties under section 2(1) IPA 2016.

CLARIFY THE APPLICATION OF THE FACTORS LISTED IN SECTION 226A(3) IPA 2024 WITH STRONGER HYPOTHETICAL EXAMPLES IN THE CODE

The IPA 2024 has three regimes for how intelligences services can examine BPDs: 1) Part 7, when an intelligence service holds the BPD itself; 2) Part 7A, when an intelligence service holds the BPD itself, but the affected individuals have a LNEP; and 3) Part 7B, when a third party holds the BPD. Annex A outlines the procedure for Part 7A authorisations related to LNEP BPDs. The IPA 2024 defines BPDs having LNEP data as "...the nature of the [BPD] is such that the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy in relation to the data." The legislation also contains factors to support the identification of a BPD containing LNEP data at section 226A(3) of the IPA 2024. These include:

(a) The nature of the data;
(b) The extent to which—
    i. The data has been made public by the individuals, or
    ii. The individuals have consented to the data being made public;
(c) If the data has been published, the extent to which it was published subject to editorial control or by a person acting in accordance with professional standards;
(d) If the data has been published or otherwise in the public domain, the extent to which the data is widely known about;
(e) The extent to which the data has already been used in the public domain.

The code lists hypothetical examples to illustrate how the factors may work in practice, a suggestion that we made in the previous consultation of the then Investigatory Powers (Amendment) Bill 2024. Hypothetical examples are highly beneficial to clarify and contextualise an entirely new category of data specific to the IPA 2024. Unfortunately, some examples are too simplistic or lack relevance, which detracts from their effectiveness. In particular, using a public telephone directory as an example, a relic from the pre-Internet era, instead of a more relevant online example, is not particularly helpful. Moreover, none of the examples address specific concerns around social media data and how the varying levels of privacy afforded to users on these platforms would affect the factors. For example, it would be useful for the code to clarify how a BPD of semi-public posts on a social media site would be treated by surveillance authorities. The Secretary of State should clarify the application of the legislative factors in the determination of LNEP BPDs.

SET CLEAR CRITERIA AND PROPORTIONAL THRESHOLDS FOR DETERMINING WHEN A DATASET QUALIFIES AS LNEP

The Secretary of State should refine the thresholds for LNEP data in sections 4.29 – 4.35 of Annex A, on BPDs containing information of "particular sensitivity." Specifically, section 4.32 states:

> "Given the nature of the datasets that may be retained and examined under Part 7A, it may not be practicable to establish during the permitted period of initial examination that

> all of the data in a dataset meets the test in section 226A(1), and a proportionate approach should be taken, particularly where, for example, a dataset is very large and an exhaustive examination is not feasible. It is therefore possible that datasets authorised under Part 7A may contain a relatively small amount of data in respect of which there is more than a low reasonable expectation of privacy."

This section raises questions about when intelligence services should use the Part 7A authorisation procedure as opposed to Part 7 for BPDs. Section 4.32 does not specify what a "relatively small amount of data" looks like empirically or what proportion of sensitive data compared to LNEP data is acceptable to allow a Part 7A authorisation.

The Secretary of State should amend the code accordingly to address this issue, such as by providing a maximum percentage of sensitive data that can be included in a BPD and still be authorised under Part 7A. Surveillance authorities can then use these thresholds to help determine which authorisation process to follow. For example, a surveillance authority might acquire a BPD containing survey responses from a public website containing a mixture of LNEP data, potentially sensitive data, and sensitive data. During the initial examination process for which no warrant or authorisation is required, the surveillance authority would use models or other tools of analysis to retrieve the specific composition of that BPD across these categories of data. The surveillance authority would then refer to the thresholds set by the Secretary of State in the codes to determine if the percentage composition of potentially sensitive or sensitive data is such that the surveillance authority can no longer consider the BPD as an LNEP BPD, and would instead make an application under Part 7.

LIMIT THE SCOPE OF NOTIFICATION NOTICES TO "RELEVANT CHANGES" THAT DEMONSTRABLY AND SIGNIFICANTLY IMPACT LAWFUL ACCESS CAPABILITIES UNDER THE LEGISLATION, SUPPORTED BY A BODY OF TANGIBLE EVIDENCE

Section 258A(1) of the IPA 2024 gives the Secretary of State the power to give a notification notice to a telecommunications or postal operator. A notification notice requires the telecommunications operator or postal operator to notify the Secretary of State of any relevant changes specified in the notice that the operator intends to make.

Annex H covers the notices regime and defines a relevant change as "a change to a service or system provided or controlled by a telecommunications operator or postal operator that would negatively impact Investigatory Powers Act 2016 capabilities and the operator's ability to provide assistance in relation to any warrant, authorisation or notice issued under the Act." The definition goes on to highlight broad examples, which include changes to:

- data retention periods by the operator,
- the operator's ability to lawfully provide communications data,
- the operator's ability to lawfully provide the content of communications, and

- decommissioning of a service.

The code includes a list of factors relevant when considering whether a change is likely to have a negative impact on the operator's technical capabilities, which would constitute a relevant change warranting the notification of the Secretary of State. Finally, the code provides a list of examples including:

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

Moreover, under the code and legislation, operators are first required to notify the Secretary of State before they make a "relevant change," and the code is vague on how the intelligence service may respond if the change is "significant." There is also the application of section 258A(12) IPA 2024 stating that an operator must be able to provide assistance in relation to any warrant, authorisation, or notice. If the change is such that the operator can no longer fulfill this obligation, the code is vague on how this would be reconciled with the company's commercial independence. In short, the Secretary of State could force companies to delay new features and services until the intelligence authority makes appropriate arrangements to maintain access to company data—delays which would negatively impact on the company's users.

The above examples, taken together with the code's definitions, are far-reaching and have the potential to cover a host of updates and core service changes. Whilst the code acknowledges that security patches would be excluded from this list, the list itself is so expansive that operators may delay changes that (a) whilst not immediately a security risk, would eventually pose a security risk, or (b) affect and strain the commercial decision-making of a company that owes a fiduciary duty to act in the best interests of the company.

To ensure a robust notification regime that does not unduly burden operators, the Secretary of State should limit the scope of "relevant change" to those that demonstrably and significantly impact lawful access capabilities under the legislation. Moreover, the narrower scope should be supported by a body of tangible evidence collected during the pre-notification notice informal and formal consultations.

LIMIT THE SCOPE OF "NEGATIVE EFFECT" FOR THE REVIEW PROCESS FOR DATA RETENTION, TECHNICAL CAPABILITY, AND NATIONAL SECURITY NOTICES

Both the legislation and the codes provide a clear appeals process for telecommunications operators, but section 11 of Annex H, which details the review process for data retention, technical capability, and national security notices, raises some concerns.

Section 11.3 begins by saying that during the review period of a notice, operators are not required to make changes to comply with the notice which they have referred to for review, and that operators can continue to make changes to their services and systems. However, the same section goes on to say that operators must not make any changes that "if implemented would have a negative effect on the capability of the operator to provide any assistance in relation to any warrant, authorisation or notice issued or given under the Act."

This review period could also be delayed by the requirement that the Secretary of State must consult or take into account the views of the Technical Advisory Board (TAB) and a JC. Whilst the review period is limited to 180 calendar days, this is still a significant period to potentially not make certain changes to services, particularly in fast-moving industries like technology.

The above provisions create a purgatory environment for operators who are, in effect, subject to the requirements of the notice because it has been issued under the legislation, despite that same notice being under review and potentially revoked if the TAB and JC consider the notice to be technically and financially infeasible and disproportionate.

The Secretary of State should update the code to limit the scope of the obligation laid out in section 11.3 by only including changes that would have "significant" or "highly critical" negative effects. A tight scoping of this obligation when a notice is under review can strike the right balance between public security interests, particularly if the notice is upheld, and the use of company resources if the notice is revoked following review.

The Secretary of State should also amend the codes to ensure that with the notice review process, JCs are empowered to consider both necessity and proportionality as part of their assessment, given that they are required to do so when assessing the initial applications for authorisation.

The code states that as part of the review process, JCs will consider the proportionality of a notice, however the codes mention both proportionality and necessity throughout. In Annex H for example, 9.11 states that a national security notice can only be given if it is necessary in the interests of national security, and the conduct required is proportionate to what is sought to be achieved by that conduct. Similarly, the Secretary of State must have regard to both necessity and proportionality considerations when deciding to issue a class BPD warrant under Part 7. Finally, any application for an individual authorisation under Part 7A must include a justification

of the necessity and proportionality of the proposed retention or retention and examination of a BPD with LNEP data. Given the equal importance the codes afford to both necessity and proportionality, it is concerning that a JC, in reviewing the legality of a notice, is only charged with considering proportionality. The Secretary of State should amend the code to ensure consistency in approach.

EXPAND GUIDANCE ON THE DECOMMISSIONING OF SERVICES, IN PARTICULAR CONFIRMING THAT THE UK GOVERNMENT WILL NOT UNREASONABLY IMPEDE ANY DECOMMISSIONING OF A SERVICE FALLING WITHIN THE NOTICE REGIME

Example 3 of section 14.11 in Annex H raises questions over the process for decommissioning a service, which is included in the code as an example of what would constitute a relevant change as discussed above. The example relates to a telecommunications operator that is decommissioning a service specified within the operator's notification notice, meaning the service is part of the list of services the Secretary of State has included as requiring notification if a relevant change takes place.

In this example, the guidance is vague on whether the government would be empowered to prevent or delay the decommissioning of the service. Indeed, it says "[n]otification of the decommissioning of a service will allow time for the government to continue to ensure public safety whilst not interrupting the commercial decisions of the company. For example, further warrants may be executed, where necessary and proportionate, within the timeframe notified before the service is decommissioned." It is unclear if further action from the government could also include the delay or prevention of the decommissioning of a service in these circumstances, and the Secretary of State should confirm this in the code, particularly to ensure the government respects the commercial decisions of a company as far as practicable and does not interfere with a company's fiduciary duties.

ENSURE THE SECTION 2(2) IPA 2016 CONSIDERATIONS ARE AFFORDED THE APPROPRIATE LEVEL OF SCRUTINY BY PUBLIC AUTHORITIES AND THAT THESE AUTHORITIES CONSIDER ALL FACTORS WHEN EXECUTING THEIR DUTIES UNDER SECTION 2(1) IPA 201

Section 2(2) of the IPA 2016 outlines four key factors the deciding public authority must have regard to when granting, denying, amending or revoking a warrant or authorisation under section 2(1) of the IPA 2016. These include:

(a) whether what is sought to be achieved by the warrant, authorisation, or notice could reasonably be achieved by other less intrusive means,
(b) whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorisation, or notice is higher because of the particular sensitivity of that information,
(c) the public interest in the integrity and security of telecommunication systems and postal services, and

(d) any other aspects of the public interest in the protection of privacy.

The code is inconsistent as to the level of consideration a deciding public authority should afford each factor in making its decision. For example, section 3.14 of Annex A specifically outlines all four factors, yet section 5.3 of the same Annex only lists (a), (b) and (d). Section 5.5 in Annex C does the same, and both sections go further than simply omitting (c), acknowledging that whilst section 2 lists another factor, consideration only applies so far as any of the factors are relevant, and that in the BPD context, (c) would rarely be relevant.

We disagree. There is a high level of public interest in ensuring the integrity and security of telecommunication systems, which include systems used daily by a significant proportion of UK users. Any modicum of distrust in the security of these systems, particularly at the hands of intelligence services, will have long-standing implications on the level of trust and scrutiny the public affords to the intelligence services, and the efforts of private businesses to maintain the highest level of privacy and security possible for the benefit of their customers. Many customers expect high levels of privacy and security from their communication services. Omittance of factor (c) from certain aspects of the code could be interpreted as a relaxation of the legislative rules and reduce the level of accountability intended by the statute.

Similarly, there is little information on how a public authority should consider the factors laid out in Section 2, which is particularly important given the above and the fact that the duty to have regard to these factors only apply insofar as they are relevant and subject to other considerations. With this in mind, the Secretary of State should reintroduce factor (c) to those areas in the code where it is missing, and the code should impose on public authorities a duty that, whilst not all factors may be relevant, they must form part of the public authority's initial consideration for authorisation, if only to confirm a lack of relevance. This would keep in line with the legislative intent, and leave no room for confusion, avoidance, or doubt as to the applicability of section 2(2).