Privacy International's Response to the Consultation on the Investigatory Powers (Amendment) Act 2024: Codes of Practice and Notices Regulations

I. Introduction

Privacy International (PI)[1] appreciates the opportunity to respond to the Government's consultation on the new and updated codes of practice and a set of notices regulations following changes made by the Investigatory Powers (Amendment) Act 2024. PI has long been troubled by the breadth of the powers in the Investigatory Powers Act 2016 (IPA). The Investigatory Powers (Amendment) Act 2024 (IPAA) only heightened our concern. We have worked in dozens of countries across the world and have followed technology policy debates in countless jurisdictions. The UK Government possesses globally unprecedented powers, some of which should not exist in a democratic society, and those that are within reason lack adequate human rights safeguards.

These draft codes and notice regulations are an opportunity to rectify and limit the ambiguity and potential for arbitrariness inherent in the IPA and Investigatory Powers (Amendment) Act. The drafts make some headway in this regard but leave significant room for improvement.

In the following submission, we respond in detail to the draft codes relating to low or no reasonable expectation of privacy BPDs ("Annex A"), third-party BPDs ("Annex B"), the retention and examination of BPDs ("Annex C"), and the notices regime ("Annex H") as well as the draft statutory instrument: The Investigatory Powers (Notification Notices, Review Periods and Technical Advisory Board) Regulations 2025 ("Annex I"). We also briefly address our ongoing concerns regarding the UK's investigatory powers regime which extend beyond the presently proposed changes to the codes and notices regulations, especially

[1] PI is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights, and the UN Refugee Agency.

given that new regulations are being laid, opening the door to further legislative changes.

We conclude our more detailed analyses with a set of recommendations we hope will be considered as the drafts are revised as following them may significantly increase the UK's compliance with human rights and international law.

II. The Draft Codes concerning Bulk Personal Datasets ("BPD") under parts 7A, 7B and 7 of the Investigatory Powers Act

This section of our response to the consultation on the IPAA codes of practice and notices regulations will focus on the Draft Codes relating to low or no reasonable expectation of privacy BPDs ("Annex A"), third-party BPDs ("Annex B"), and the retention and examination of BPDs ("Annex C").

The below submissions are without prejudice to our position that the current power to obtain BPDs under part 7 of the IPA constitutes a disproportionate and unlawful interference with the fundamental right to privacy.[2] Similarly, we maintain our position that the low or no reasonable expectation of privacy BPDs ("Low Privacy BPD") and third-party BPDs ("3PD") raise additional concerns in addition to those we have articulated in relation to part 7 BPDs.

With respect to the definition of Low Privacy BPDs inserted by the IPAA, we consider that this runs counter to longstanding principles of privacy law and omits crucial safeguards to prevent abuse, as required by the European Convention on Human Rights ("ECHR").[3] With respect to the new 3PD regime, we consider that this may allow intelligence services to access data that has been collected or processed contrary to the law and fails to provide for the proper management of third-party BPDs.[4] We do not propose to repeat in detail the reasoning for our general positions as regards the relevant BPDs, but instead place reliance on the materials referenced below.

Annex A

We remain concerned that Low Privacy BPDs could facilitate the mass collection of publicly available data, including social media data such as written posts, videos, and images among other forms of personal data.[5] This is because the Low Privacy BPD definition and the relevant criteria pursuant to section 226A(3) of the IPA weaken existing privacy and data protection standards. When assessing what constitutes a low privacy BPD, the intelligence services can consider a number of factors – the majority of which relate to the public nature of the data, including

[2] PI's submission in advance of the consideration of the eight periodic report of the United Kingdom to the UN Human Rights Committee, 140th session, February 2024, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/DownloadDraft.aspx?key=1cJsGKycgclvjlmzvk3XZBJLEEuJ0pUZA4SmTMgjjR53+CyhCHkGSuTw0gfZYBCpmlbfE0i8kfchCkr+4KrWvQ==
[3] PI's Response to the UK Government's Investigatory Powers (Amendment) Bill, 22 February 2024, https://privacyinternational.org/advocacy/5258/pis-response-uk-governments-investigatory-powers-amendment-bill
[4] *ibid.*
[5] *ibid.*

the extent to which it is known about and has previously been used. This creates a false equivalence between the availability of the personal data, including how it is obtained, and the privacy protections it attracts.

In the case of publicly available social media data, this will frequently be no less sensitive than that which is obtained through covert social media monitoring. Even if it is made public by an individual, it may contain personal data relating to political opinions (which is likely to be of particular interest to the intelligence services).[6] While section 226A(3)(a) includes consideration of the nature of the data in question, this is one factor weighed against four others that relate to the public quality of the data tilting the balance.

We submit an individual's reasonable expectation of how their data will be processed if they publish something publicly is unlikely to include further use by the intelligence services as part of a Low Privacy BPD. A fact and context specific assessment of the reasonable expectations of a data subject as regards how their data will be used is critical to determine if a measure interferes with data protection principles and the right to privacy. For example, in *Halford v. UK* – the European Court of Human Rights ("ECtHR") underlined that a "a reasonable expectation of privacy is a significant though not necessarily conclusive factor" in deciding whether there has been an interference with the right to privacy.[7] The accepted role of an individual's reasonable expectation of privacy in both the right to privacy and data protection law is at odds with Low Privacy BPDs. This is because they are collected on a bulk basis and therefore cannot incorporate an individual's assessment of their reasonable expectation of privacy; and they assume that a data subject who published data on social media has a low expectation of privacy in relation to that information.

Lack of legal certainty around contents of Low Privacy BPDs

Before coming into force, the deliberations around the shape of the IPAA were characterised by a fundamental lack of clarity around what information could fall within the new Low Privacy BPD. For example, during a parliamentary debate on 11 December 2023 the Parliamentary Under-Secretary of State within the Home Office stated that a Low Privacy BPD could consist of a collection of news articles.[8] Similarly, the Explanatory Notes to the Bill referred to Low Privacy BPDs as potentially consisting of online encyclopaedias.[9] Clarity as regards what data can be collected within a Low Privacy BPD was sought by the Joint Committee on Human Rights in a letter to the SoS in response to concerns raised by PI and other civil society organisations:

> *There is perhaps some ambiguity or confusion as to what data is envisaged to be caught by these provisions. For example, is it merely*

[6] PI's Response to the UK Government's Investigatory Powers (Amendment) Bill, cited above.
[7] ECtHR, *Halford v UK*, App no 20605/92, Judgment, 25 June 1997, §45.
[8] Investigatory Powers (Amendment) Bill [Lords], 7 March 2024, second reading, col. 1743, https://hansard.parliament.uk/lords/2023-12-11/debates/AC2BC51B-045E-47F0-90C5-893B853334EB/InvestigatoryPowers(Amendment)Bill(HL)
[9] Investigatory Powers (Amendment) Bill [HL], Explanatory Notes, 31 January 2024, https://publications.parliament.uk/pa/bills/cbill/58-04/0157/en/230157en.pdf

online encyclopaedias, Companies House registers or news articles; ***or would it also cover, for example, quite extensive discussions over the internet or mass voice or face images, as has been mentioned in evidence****? Discussions online often disclose sensitive information (whether about the individuals themselves or a person they are talking about) such as an individual's sexual orientation, political opinion, religion, health status or potentially sensitive information about children. The requisite clarity about the scope of these measures is currently not available from the face of the Bill. Greater clarity would be helpful to understand the sorts of things within and outwith the scope of this category, and in improving transparency and confidence in this process. Could you please provide this clarity as to the sorts of information that would, and would not, fall within the scope of the "low or no reasonable expectation of privacy" bulk personal dataset.*[10] (emphasis added)

The government's response to the concerns raised by the JCHR did not properly engage with this issue.[11] The government merely re-stated the statutory criteria as regards when a dataset could be classified as a Low Privacy BPD. This does not provide clarity, but by contrast underlines exactly the breadth of the power under section 226A(3) of the IPAA and the vast scope of the information that could be gathered pursuant to it.

The response to the concerns of the JCHR stated that: "*absent some exceptional circumstance, it is highly unlikely that a dataset containing data as sensitive as health records would ever be considered a dataset in respect of which there is a low or no reasonable expectation of privacy.*" This fails to address several of the above categories of data raised by the JCHR including social media data (such as voice and image data collected from social media platforms). The response goes on to cite protections under section 226D as a relevant safeguard, which will mitigate the risk that potentially sensitive information is collected. As set out in Annex A, this provision comes into play if information with more than a low expectation of privacy is identified within the BPD. If this takes place the intelligence service must then treat that part of the dataset as if the relevant authorisation had been cancelled, it must be removed and deleted, or a Part 7 warrant must be sought in relation to it.

The section 226D safeguard depends on the IPA and Annex A providing sufficient clarity and foreseeability as regards when information will not be regarded as low/no privacy data. This is not provided for by the current iteration of Annex A. Annex A reiterates the relevant statutory requirements and emphasises that any assessment of whether information is low/no privacy must be undertaken in the round. As set out in our previous submissions, a holistic assessment based on the factors set out in the status is likely to lead to the regular collection of sensitive information.

[10] Joint Committee on Human Rights, Letter to Parliamentary Under-Secretary of State, 6 March 2024, https://committees.parliament.uk/publications/43763/documents/217255/default/
[11] Home Office, Response to JCHR, 19 March 2024, https://committees.parliament.uk/publications/44016/documents/218055/default/

For the avoidance of doubt given the lack of clarity around the meaning of sensitive data in the context of Low Privacy BPDs, we place reliance on the framing of sensitive data under data protection law and the human right to privacy. Under Article 9 of the GDPR, special categories data are recognised as requiring a heightened level of protection due to their sensitivity. Special categories data includes that which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[12] As set out above, social media information may fall within the definition of a Low Privacy BPD notwithstanding the likely presence of data that reveals political beliefs as well as biometric data (by way of two non-exhaustive examples).

Annex A goes on to state that:

> *In some countries different types of data are treated as private or non-private depending on the laws of that country (such as company ownership or land ownership information). Furthermore, in some countries it is commonplace for data on citizens' lives to be regularly and routinely accessed at scale.* ***For example, datasets containing personal data may be made available, either for free or for a payment, on public forums. This will be a relevant consideration when deciding whether section 226A applies****. (emphasis added)*

This appears to be the closest yet to an admission that that information available through social media could be collected in a Low Privacy BPD. Annex A also conflates information being made public with its sensitivity. This conflation is clearly articulated when the code suggests that confidential material may no longer be sensitive once it is made public:

> *"A low/no BPD could contain sensitive personal data (see section 202), health records, or confidential material relating to sensitive professions, but only where the information is no longer sensitive. For example, a communication between a lawyer and client might have become public in circumstances in which it has lost its necessary quality of confidence: a dataset containing this type of information could meet the test in section 226A(1) and be retained in a low/ no BPD."*

While the response to the JCHR stated that the section 226D safeguard would mitigate against the risk of sensitive information being collected, Annex A notes that that low privacy BPDs may include sensitive information, but that small proportions of such data should not change the overall character of the BPD including its status as a low/no privacy BPD. This is said to be on the circular basis of the section 226D safeguard. The section 226D safeguard relies on such data

[12] We note that Article 8 ECHR has similarly recognised certain special categories of data as requiring a heightened level of protection. See for example, ECtHR, *Glukhin v Russia*, App no 11519/20, Judgment, 4 July 2023, §76: "Personal data revealing political opinions, such as information about participation in peaceful protests, fall within the special categories of sensitive data attracting a heightened level of protection."

being detected, which is unlikely to take place until substantive examination. Given the potential size of BPDs and the fact that individual authorisation can be bypassed where a dataset falls within an approved category, there is no way that necessity and proportionality can be adequately assessed for each kind of data at the time that approval is granted. This in effect renders the relevant safeguards nugatory.

Annex A also inhibits the proper application of section 226D even once a Low Privacy BPD is examined. This is because the starting point in Annex A is that a low privacy BPD is "highly unlikely to contain information of particular sensitivity". As such, once a low privacy BPD is obtained the possibility that it contains information that falls outside of the statutory definition at 226A(3) is unlikely to be considered. This contradictory position is incompatible with the in accordance with the law criterion for the purposes of Article 8 ECHR.

In order for an interference to be in accordance with the law, it must have "some basis in domestic law," and it must be "compatible with the rule of law," which means that it should comply with the twin requirements of "accessibility" and "foreseeability", and it must contain sufficient constraints against arbitrary or disproportionate use.[13]

The principle of "foreseeability" means that the domestic legal framework (which includes a public authority's published policies) must "*give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention.*"[14] Further, that legal framework "*must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise*".[15]

The Low Privacy BPD regime cannot meet these requirements for the following reasons:

- As per the JCHR's letter and the concerns we raised in our response to its call for input, the categories of data that could fall within a Low Privacy BPD are insufficiently clear.
- The meaning of sensitive data contained in Annex A conflicts with established jurisprudence of the ECtHR. For example, in Peck v. UK – disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras constituted a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time. Notably, this assessment rested on the assumption that the applicant could not

[13] For example, *R (Bridges) v Chief Constable of South Wales Police* [2020] 1 WLR 5037 (CA), §80.
[14] ECtHR, *Fernandez Martínez v Spain* [GC], App No 56030/07, Judgment, 12 June 2014, §117; see also ECtHR, *Big Brother Watch and others v UK* [GC], App No 58170/13, 62322/14 and 24960/15, Judgment, 25 May 2021, §333.
[15] ECtHR, *S & Marper v UK,* App Nos 30562/04 and 30566/04, Judgment, 4 December 2008, §95.

reasonably have expected that his data would be used this way even if their actions were "already in the public domain".16

- The starting point adopted in Annex A that a low privacy BPD is highly unlikely to contain sensitive information is contradicted by an admission in the same policy that datasets may in fact include such information.
- Such information is unlikely to be routinely identified until the dataset is examined. This is with reference to the potential size of datasets and the nature of the authorisation process, including the possibility for datasets to be authorised by way of a category authorisation. We submit that it is impossible for there to be adequate consideration of proportionality and necessity in these circumstances particularly when the starting point is that Low Privacy BPDs are highly unlikely to contain sensitive information.

At a minimum, Annex A must make clear what categories of data will not be gathered as part of a Low Privacy BPD. With respect to hacked and/or stolen information that is then made public, the government made clear during the second reading of the IPAA that such information would not fall within a Low Privacy BPD. Given this commitment, it is unclear why the code cannot clarify that this and other categories of data will not be contained within Low Privacy BPDs.

Low privacy BPDs and machine learning

We are particularly concerned by the suggestion in Annex A that Low Privacy BPDs will be used to build and test machine learning models:

> *However, in some cases, the use to which the data will be put may have an impact on the assessment of reasonable expectation of privacy: for example, when using data for capability development such as building and testing machine learning models. This may mean that some data that would not routinely be assessed as having a low reasonable expectation of privacy may come within scope of Part 7A if the sole use of the data will be for capability development.*

Firstly, we submit that the use of the data should not be a relevant consideration in favour of collecting data for use as a Low Privacy BPD. Privacy considerations are not assessed with regard to the utility of certain information for the intelligence services, but rather from the starting point of what the expectations of individuals subject to certain processing operations are likely to be. Given that the very definition of a BPD includes the processing of information not of interest to the intelligence services, the use of personal data by the intelligence services may be entirely unforeseeable to individuals whose data falls within a BPD. In the case of personal photographs and reflections posted to social media, an individual may have a high expectation of privacy in relation to the information in question.

The suggestion from the above is that certain Low Privacy BPDs are likely to be used for the sole purposes of building and testing machine learning technologies. There is no mention of the same in Annexes B and C. The categories of data that can be processed for the purpose of building and testing machine learning

[16] ECtHR, *Peck v UK*, App no 44647/98, Judgment, 28 January 2003, §§61-62.

models is even more opaque than the information that may generally fall within a Low Privacy BPD. It appears from Annex A that the sole criterion is data that would not routinely be assessed as having a low reasonable expectation of privacy, which risks the processing of sensitive information that may otherwise fall outside of the Low Privacy BPD definition.

The rationale for this appears to be that using information for the development of machine learning models is somehow less intrusive since the data is not being directly processed for operational purposes (notwithstanding the fact that outputs of machine learning models may be used in an operational context as addressed with reference to Annex C below). Below we address why this rationale is flawed.

It is well established that machine learning systems, which are underpinned by training data, are highly data intensive.[17] In the intelligence context this is likely to spur an increase in the authorised collection of data as was raised as a concern by a lawyer interviewed for the Centre for Emerging Technology and Security's research report on Privacy Intrusion and National Security in the Age of AI.[18]

Building and testing machine learning models is likely to involve the use of personal data for training purposes. Given the similar nature of the technology at play, the deployment of Low Privacy BPDs for machine learning purposes is analogous to the use of publicly available data for training purposes of AI models in the commercial context. Such data processing is taking place in ways that cannot be reasonably predicted by the owners and producers of this data.[19] The training of commercial AI models is happening almost entirely in secret with leading AI companies showing reluctance to be transparent about their activities.[20] In this context, the ICO has stated that the "*processing of personal data to develop generative AI models is likely to be beyond people's reasonable expectations at the time they provided data to a website*"[21] and that "*common practice does not equate to meeting people's reasonable expectations … particularly when it comes to the novel use of personal data to train generative AI in an invisible way or years after someone provided it for a different purpose (when their expectations were, by default, different)*".[22]

The present lack of transparency about the scraping of personal data for AI training purposes is likely to be contrary to the GDPR. In fact, both the ICO and the European Data Protection Board (EDPB) have recently produced guidance that

[17] PI, 'Large language models and data protection', 14 August 2024, https://privacyinternational.org/explainer/5353/large-language-models-and-data-protection
[18] Centre for Emerging Technology and Security, 'Research Report: Privacy Intrusion and National Security in the Age of AI, Assessing proportionality of automated analytics', May 2023, https://cetas.turing.ac.uk/sites/default/files/2023-05/cetas_research_report_-_proportionality_and_intrusion_final_0.pdf
[19] 'PI response to ICO consultation on data subject rights and generative AI', 2 July 2024, https://privacyinternational.org/advocacy/5338/pi-response-ico-consultation-data-subject-rights-and-generative-ai
[20] *ibid.*
[21] *ibid.*
[22] Information Commissioner's Office response to the consultation series on generative AI, https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/response-to-the-consultation-series-on-generative-ai/tackling-misconceptions/

emphasises the importance of transparency. The ICO stated that "*we expect generative AI developers to significantly improve their approach to transparency*"[23] and the EDPB have remarked that "*simply because information relating to the development phase of an AI model is included in the controller's privacy policy, it does not necessarily mean that the data subjects can reasonably expect it to happen; rather, this should be analysed … on the specific circumstances of the case and considering all of the relevant factors.*"[24]

Of relevance in the intelligence context is the difficulty in being able to erase personal information that has been used as training data (therefore to meet the right of erasure and limits on data retention). This is because personal information is held within the parameters of a model in addition to more traditional form (such as a database) and as such it is not obvious how the data can be identified, corrected, or deleted.[25] As set out above, the sole safeguard as regards the processing of sensitive information and data that would not otherwise fall within a low privacy BPD relies on the possibility of identifying such information and removed or deleting it. This is unlikely to be completely possible in the machine learning context in which the information in question cannot be isolated from the AI model into which it has been absorbed without damaging the model.[26]

Before authorising a low privacy BPD through either an individual or category authorisation, the relevant authority must conduct a necessity and proportionality assessment. As Annex A correctly notes, this requires an assessment of whether there are less intrusive alternatives to achieve the same aim. It is unclear how an assessment of less intrusive alternatives and necessity and proportionality more generally can take place in the machine learning context. This is because the less intrusive alternative is simply not to use bulk datasets for model development and training purposes. Yet far from promoting this alternative, Annex A inhibits giving officials the option to collect more sensitive information than would otherwise come within Low Privacy BPDs if used solely for machine learning.

Given the substantial interference with the right to privacy of anyone whose personal data is used for machine learning purposes, it is highly concerning that this has been introduced via the backdoor through the relevant Code of Practice rather than regulated via an explicit and discrete power in the Investigatory Powers Amendment Act. Without a clear legal basis and distinct Code of Practice that establishes (a) what data will used for these purposes; (b) how sensitive information that would otherwise not fit within a low privacy BPD could be erased or removed from the dataset once deployed for training purposes; and (c) how proportionality and necessity can be assessed (including consideration of when it

[23] *ibid.*
[24] EDPB, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models' (17 December 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en
[25] 'PI response to ICO consultation on data subject rights and generative AI', 2 July 2024, https://privacyinternational.org/advocacy/5338/pi-response-ico-consultation-data-subject-rights-and-generative-ai
[26] European Parliamentary Research Service, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence', June 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf, §3.5.2.

would not be appropriate to use datasets for this purpose) we submit that Low Privacy BPDs should not be used to train and develop machine learning models.

Annex B

We remain concerned that 3PDs could detrimentally impact the right to privacy. The IPAA is likely to facilitate the purchase of or direct access to the personal data of unlimited numbers of people from data brokers and other actors.[27]

Data broker Experian already provides services to a number of UK police and law enforcement agencies through its 'Investigator Online' platform[28] and we are concerned about further growth in this practice, which is regularly deployed in the US and is extremely intrusive given the extensive and granular nature of personal data collected by actors such as data brokers.[29] Such data can include an individual's real time location, their IP address, or sensitive information relating to the websites a person visits (such as if they visit a website about the provision of abortion services).[30] Data examined through a third-party BPD warrant can therefore also constitute a serious interference with the right to privacy.

As the powers are framed, we consider that 3PDs would enable the intelligence services to collect and use stolen or otherwise unlawfully processed data, which has profound implications for the in accordance with the law requirement pursuant to Article 8 ECHR as well as public law principles.[31] With regard to the in accordance with the law requirement, we note that the ECtHR has previously held that if a measure breaches another legal provision this may render it not in accordance with the law (without the need for the usual substantive consideration of the test outlined above).[32]

In our submissions responding to the JCHR's call for input on the IPAA we argued that the scope and manner of exercise of the powers relating to 3PDs also lack sufficient clarity. The publication of Annex B has further solidified both these concerns. The lack of clarity regarding what data can collected by way of a 3PD must be remedied given the potentially highly intrusive data collection practices of actors such as data brokers from whom access to datasets could be purchased through the new 3PD powers.

Lack of clarity around exercise of powers relating to 3PDs

The starting point in the IPAA is that the third-party is any person other than the intelligence services. While it may be impractical to list each body or individual that could constitute a third-party in the code, the suggestion in Annex B that this

[27] PI's Response to the UK Government's Investigatory Powers (Amendment) Bill, cited above.
[28] gov.uk Digital Marketplace, 'Experian Tracing Solutions for Police and Law Enforcement with Investigator Online' https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/485058705009061
[29] PI's Response to the UK Government's Investigatory Powers (Amendment) Bill, cited above.
[30] *ibid.*
[31] *ibid.*
[32] See for example, ECtHR, *Blyudik v Russia,* App No 46401/08, Judgment 25 June 2019, §75 in which the Court found that the breach of the right to liberty as protected by Article 5 ECHR breached the in accordance with the law requirement for the purposes of Article 8§2.

"*may include individuals, companies, government departments or other public authorities*" is insufficiently clear. As set out above, the government stated during the second reading of the IPAA that Low Privacy BPDs would not comprise of stolen information (even as such a commitment has not been included in Annex A). No equivalent commitment of any kind has been made in the context of the 3PDs.

This is concerning given that Annex B suggests that the powers inserted by part 7B of the IPAA would include a scenario where "*a commercial company provides privileged access to an intelligence agency so additional data is made available to that agency over and above that which could be purchased by another client.*"

We submit that Annex B should rule out obtaining 3PDs from certain actors including those who have collected stolen or hacked information or who have processed personal data unlawfully (and the associated information in such datasets). This is something that would both ensure compliance with the in accordance with the law requirement for the purposes of Article 8 while also safeguarding the veracity and probity of the information obtained. In the alternative, there are real risks that the intelligence services could collect inaccurate or misleading information when purchasing data from private actors for whom it may be particularly easy and cheap to produce false data.[33]

While the IPAA requires a necessity and proportionality assessment as part of the authorisation process, we consider that this must also incorporate an assessment of the compliance of the data obtained from the relevant third-party with data protection legislation prior to examination. Annex B should require that this assessment be undertaken by a legal adviser within the intelligence services. We note that Annex B already requires an assessment of lawfulness by a legal adviser where there is any "*doubt as to the lawfulness of the proposed handing or dissemination*" of information concerning constituency business of a Member of Parliament.

The assessment of the lawfulness of the data obtained is vital in the context of 3PDs given the fact that the new 3PD power contained in the IPAA would appear to authorise the intelligence services accessing information collected by actors such as data brokers who have on multiple occasions been found to breach data protection law. For example, on 16 January 2024, the Belgian DPA sanctioned a data broker for violating several provisions of the GDPR.[34] The data broker had obtained the information from several sources and then sold it to interested third parties largely for advertising purposes. The violations found by the DPA were systemic and systematic and related to the company's very business model. They included a violation of the necessity and balance of interest tests, the data minimization principle, and the requirement to notify data subjects of the processing in violation of Article 14 of the GDPR. Irrespective of an assessment of

[33] Stiftung Neue Verantwortung, 'Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?', November 2022, https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier

[34] Covington, 'Inside Privacy: Updates on Developments in Data Privacy and Cybersecurity, Belgian Supervisory Authority Sanctions Data Broker', 22 January 2024, https://www.insideprivacy.com/advertising-marketing/belgian-supervisory-authority-sanctions-data-broker/

the lawfulness of the intelligence services purchasing access to information from data brokers, it remains unclear to us how data brokers (and other companies processing data for commercial purposes) can comply with their own obligations under the provisions of the GPDR and equivalent legislation when they provide intelligence agencies with access to the information they have gathered.

Finally, we note that there is nothing in Annex B that provides chain of custody safeguards around in situ access to information held by a third-party. There is an urgent need for the code to address the conditions of access, including how access will be granted, how the intelligence services will ensure that data is not copied over to their own systems during and following examination, and how access will be terminated following the refusal, expiry, and/or non-renewal of a 3PD warrant.

Annex C

PI has long objected to the disproportionate collection and use of BPDs by the intelligence services, as described in more detail at the end of this submission. Our comments here are without prejudice to the arguments we have brought forward in previous legal challenges and advocacy submissions.

The use of machine learning technology for the examination of BPDs

Annex C references the use of "*automated systems… to effect the selection for examination in accordance with section 221 of the Act and the arrangements made by the Secretary of State under that section for ensuring that any selection of data from the BPDs is carried out only for the specified operational purposes.*" Annex A is the sole Draft Code that references the use of datasets for the development and training of machine learning models. There is therefore an urgent need for clarifications as regards whether Low Privacy BPDs would be used to train automated systems that select data for examination by the intelligence services. This is with reference to the substantial interference with Article 8 ECHR arising from both the collection of Low Privacy BPDs (addressed above) and the examination of data under part 7 of the IPA.

Recommendations

Annex A

1. Annex A must make clear what categories of data will not be gathered as part of a Low Privacy BPD.

2. While we raised the absence of a discrete legal basis and Code of Practice for the use of BPDs for machine learning purposes above, at a minimum we consider that Annex A must confirm whether personal data contained in a Low Privacy BPD will be used to train machine learning models. It should also provide confirmation as regards what categories of data will be used for such purposes; how sensitive information that would otherwise not fit within a Low Privacy BPD would be erased or removed

from the dataset once deployed for training purposes; and how proportionality and necessity can be assessed (including consideration of when it would not be appropriate to use datasets for training purposes).

3. If the above information is not provided, we consider that personal data contained within Low Privacy BPDs should not be used to train and develop machine learning models.

Annex B

4. Where access to a 3PD is likely to involve the intelligence services examining personal data, the authorisation process should include an assessment of the lawfulness of the information to be accessed, in particular its compliance with data protection legislation. This assessment should be carried out by a legal adviser within the intelligence services.

5. Where personal data is likely to have been processed unlawfully by the third-party it should not be accessed or examined by the intelligence services.

6. Annex B should set out the conditions under which access to a 3PD will be granted, how the intelligence services will ensure that data is not copied over to their own systems during and following examination, and how access will be terminated following the refusal, expiry, and/or non-renewal of a 3PD warrant.

Annex C

7. Annex C should clarify whether Low Privacy BPDs would be used to train automated systems that select data within part 7 BPDs for examination by the intelligence services.

III. The Notices Code of Practice

Privacy International continues to be deeply concerned about the existence and operation of the notices regime in the UK under the Investigatory Powers Act 2016 (IPA). We have worked in dozens of countries across the world and have followed technology policy debates in countless jurisdictions. The UK Government possesses globally unprecedented powers, some of which should not exist in a democratic society, and those that are within reason lack adequate human rights safeguards.

Both the inherent nature of notices and the way that the UK has implemented the regime create a troubling and destabilising effect on privacy, online security and human rights in the UK. The use of notices (and the threat of their use) has wide-reaching and systemic impacts. They negatively affect the proper functioning of the telecommunications sector; the reputation of the UK with respect to global communications networks; and the security of connected devices.

The very purpose of notices is to facilitate intrusive practices that undermine people's rights. But the present safeguards against these threats are insufficient. Furthermore, the UK's approach has not caught up with and responded to changes in the international context relating to end-to-end encryption since 2018, threatening to undermine the compliance of the UK regime with norms of international law.

Background: the profound security and privacy implications of the notices regime

Data Retention Notices (DRNs), National Security Notices (NSNs) and Technical Capability Notices (TCNs) can be used to require telecommunications operators to carry out activities that would facilitate intrusive forms of surveillance - such as interception and equipment interference - that impinge people's rights. They can also be used to undermine the security of both targeted devices and any other devices using the same products and services. For example, a notice could require the sending of false security updates or refraining from fixing a security vulnerability, or in general to alter equipment that an operator owns or the security of the services they provide.

The impact of the notices regime is systemic and far-reaching. That is because a notice can demand that operators alter their services in a way that affects ***all users***. For instance, a TCN requiring a telecommunications operator to remove electronic protection could be used to force a company such as Meta or Apple to remove or undermine the end-to-end encryption (E2EE) of services such as WhatsApp or iMessage with ***global*** effect, potentially undermining the security of the Internet as a whole. Given that some of the companies which could be targeted by notices provide systems used by millions or billions of people, the impact of a forced change to such systems would be incredibly far reaching.

This systemic impact in fact reaches even further. The very presence of the notices regime disrupts the relationship between users and companies. That relationship

is based primarily on trust: people have to trust that their devices, networks and services are kept safe from unintended errors, bugs or vulnerabilities that can be exploited by third parties. It is a constant struggle for software developers and testers to discover and fix these bugs before they are used for malicious purposes. In contrast, equipment interference often depends on exploiting vulnerabilities in systems to facilitate a surveillance objective. It may also involve manipulating people to interfere with their own systems, such as could be accomplished by a false security update. These techniques betray users' trust, the loss of which can undermine the security of systems, and the internet as a whole.

In addition, because of their systemic and global implications, notices entail a significant interference with the business operations of telecommunications operators. They ultimately entail the government directing the activities of private businesses (including by requiring the creation of dedicated systems, processes or facilities) against the privacy and security interests of their customers. That is problematic, and harmful to the UK's international reputation.

Intrusive measures like notices erode peoples' rights to privacy, to freedom of expression and to freedom of association. They constitute the co-option of private actors in state surveillance of citizens, an encroachment on people's freedom and a constraint on our free society. They can also undermine the security of online communication as a whole by allowing security flaws to remain unaddressed, or even by creating them in the first place. The privacy and security implications of the UK notices regime are profound.

Given this, we would expect there to be clear and robust safeguards over the use of notices. While some safeguards exist, we believe the Code currently being consulted on, as well as other relevant legislative material, to be inadequate. The current regime and the proposed Code of Practice permit notices to be used for an excessively broad range of applications and purposes. More concrete restrictions are needed – in the Code, but also in the regulations – that limit the purposes for which notices can be sought. While many of these concerns are longstanding flaws of the notices regime, developments in international law since the Code was first drafted in 2017 provide fresh impetus for law and practice to be revised.

The Code claims that it "sets out further detail on the circumstances in which a data retention, technical capability, national security, or notification notice can be given, the obligations that may be imposed by the giving of a notice and the ensuing right of review" [1.2]. However, in practice it fails to provide adequate parameters or limitations on what notices can be used for, thus failing to protect human rights, online security and comply with international law.

Overarching duties

Section 2 IPA

In a number of places, the Code refers to the overarching obligations found in section 2 IPA (eg at paras 3.2, 4.23, 7.4, 7.14, 9.18). These general duties require a public authority to have regard to, inter alia, the following:

- whether what is sought to be achieved by the warrant, authorisation or notice could reasonably be achieved by other less intrusive means,
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

And, where relevant, to:

- other considerations which are relevant to—
    - whether the conduct authorised or required by the warrant, authorisation or notice is proportionate, or
    - whether it is necessary to act for a purpose provided for by this Act,
- the requirements of the Human Rights Act 1998, and
- other requirements of public law.

However, the Code does little to build on these general obligations. The high point is in para 7.15, which states that when considering the public interest in the integrity and security of telecommunications systems (when giving a TCN), particular reference should be made to any obligations relating to the removal of encryption in a TCN. But that should go without saying. Paras 4.24 and 9.19 (in relation to DRNs and NSNs) add nothing to the overall requirements but merely restate them.

In any case, we do not believe that the section 2 general duties provide sufficient safeguards against the potential harms of notices. That is because, firstly, the duties are merely to 'have regard' to these important considerations – a standard which does not guarantee that they will be fully and properly addressed. The lack of transparency in the regime provides little comfort that they are being so. In any case, obligations under the Human Rights Act and everyone's right to private life (not merely the public interest in the protection of privacy) must be complied with, not simply taken into account. Secondly, the Code fails to flesh out in any detail what the concrete implications of these overarching duties might be in practice.

Section 255 IPA

Section 255(3) of the Act sets out considerations that the SoS must take into account before giving an NSN or TCN. However, both para 7.13 and 9.17 misrepresent the provisions of the Act and provide for an unbalanced reading of s255(3) IPA. That is because:

- Para 7.13 opens the door to including speculative "projected" benefits into the calculation;
- Para 7.13 re-introduces the concept of benefits into consideration of the likely number of users to be affected by a notice. There is no basis for doubling up the consideration of benefits in this way in the Act, and no

reason for thinking that the number of users relates only to benefits and not also harms. The Code should also explicitly recognise (for both NCNs and TCNs) that the likely number of users includes people from outside the UK;
- The cost of complying with a notice is interpreted as only meaning the direct financial costs of complying with a notice in both paras 7.13 and 9.17. The Code (and the SoS) should also consider the wider costs an imposition of a notice might have for an operator and its users. This will include the potential chilling effect for users within and outside the UK, the impact on business operations, and costs stemming from litigation brought by the operator and/or users against the UK Government;[35]
- Para 9.17 omits the "technical feasibility" factor without any justification.

Finally, several of the factors contained in the Code require the Secretary of State to consider them with reference to representations made by operators only. It would be more appropriate if the Secretary of State also considered any relevant representations made by independent regulators, such as the ICO or Ofcom, that might provide further insight.

In various places, the Code treats the same obligations differently when they appear in different places. It is not clear what the intended effect of this is. If different interpretations are meant for different notices, then this should be stated explicitly and justified.

Technical Capability Notices

For TCNs, the Code notes that "the only obligations that may be imposed by a [TCN] are those set out in regulations" (para 7.4, see also para 8.1). However, the relevant regulations are excessively broad and open-ended and do not contain any explicit limitations on what a TCN can be used for. Obligations such as the below could be used to undermine encryption or prevent vital security patches and updates:

- "to provide and maintain the capability to … remove electronic protection applied by or on behalf of the telecommunications operator to the data where reasonably practicable";[36]
- "to ensure that any apparatus, systems or other facilities or services necessary to obtain and disclose communications data are of a reliability specified in the notice";[37]
- "to install and maintain any apparatus provided to the operator by or on behalf of the Secretary of State for the purpose of enabling the operator to obtain or disclose communications data".[38]

[35] The ECtHR has found that individuals located abroad can still claim victim status under the Convention, and accordingly bring a claim against the UK Government, if they have been subject to surveillance. See ECtHR, *Wieder and Guarnieri v the United Kingdom*, App Nos 64371/16 and 64407/16, Judgment, 12 September 2023, §94.
[36] The Investigatory Powers (Technical Capability) Regulations 2018 (SI 2018/353), Schedule 2, Part 1, §9(b).
[37] *ibid*, §3.
[38] *ibid*, §110.

The Code fails to provide any further detail or information about these requirements (in fact the information in para 7.5 is less detailed than in the regulations).

The capability to remove encryption undermines security and privacy

A TCN may require an operator to remove electronic protection applied by or on behalf of that operator to any communications or data. Paragraph 7.6 of the Code further states:

> *An obligation imposed by a technical capability notice on a telecommunications operator to remove encryption does not require the operator to remove encryption per se. Rather, it may require that operator to maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation.*

Together with paragraphs 7.7 and 7.8, this appears designed to assuage concerns about TCNs being used to undermine encryption. But they do not succeed in this effort. Any apparent distinction between "removing encryption per se" and "maintaining the capability to remove encryption" is irrelevant, since maintaining that capability entails undermining the security and privacy of the system as a whole.

The mathematical nature of end-to-end encryption (E2EE) means that maintaining any such capability inherently compromises the security of the whole telecommunications services and the confidentiality of all users' data, even before any removal of encryption actually takes place. This is because:

> *Law enforcement demands for exceptional access … will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend. The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict. The costs to developed countries' soft power and to our moral authority would also be considerable.*[39]

Removing this protection would not only place a disproportionate burden on operators, but would also result in disproportionate negative consequences for users and their rights, rendering thus the serving of any such notice impossible.[40] A notice along the lines envisaged in paragraph 7.6 would impose a generalised obligation upon an operator to pre-emptively and indiscriminately maintain access to users' encrypted communications. The SoS could then serve a warrant upon an operator (who would have likely already been served with an earlier, general warrant to retain all encrypted communications) to access and/or disclose communications pertaining to specific individuals.

---

[39] Harold Abelson, Ross Anderson and thirteen others, 'Keys under doormats: mandating insecurity by requiring government access to all data and communications' (2015) 1 *Journal of Cybersecurity* 69, 78.
[40] See also PI, 'Securing Privacy: PI on End-to-End Encryption', 2022 https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption

Even if it were possible to remove encryption only for certain communications, a general obligation imposed upon an operator to "maintain the capability to remove encryption" in effect amounts to a general warrant, which are normally prohibited under common law, going back 250 years. As recently confirmed by the High Court:

> *The aversion to general warrants is one of the basic principles on which the law of the United Kingdom is founded. As such, it may not be overridden by statute unless the wording of the statute makes clear that Parliament intended to do so.*[41]

Indiscriminate measures such as these are also incompatible with international and EU human rights law. The ECtHR has underlined that using blanket or indiscriminate measures "fails to strike a fair balance between the competing public and private interests".[42] The same conclusion that general measures are incompatible with human rights law has also been reached repeatedly by the European Court of Justice in cases dealing with measures mandating the general or indiscriminate retention of communications data.[43]

Para 7.15 likewise does little to prevent the dangerous and unlawful use of TCNs to undermine encryption. It is ambiguously framed and phrased and could be interpreted in a number creative ways that could be used to undermine encryption for users.

Necessity and proportionality

The wording on necessity and proportionality for TCNs is overly compressed – comprising only the first sentence of para 7.16. The Code therefore fails to provide any meaningful insight into how these safeguards ought to function to protect people's rights.

Reasonably practicable

In several places, both the Code and the regulations refer to TCNs as only containing requirements that are 'reasonably practicable'. However, without any further information as to what sorts of measures are to be considered reasonably practicable (or not) and on what basis that decision will be made, this does not function as a satisfactory or meaningful safeguard.

In fact, the potential interference with an operator's business operations is significant. They may require the creation of dedicated systems, considerable costs, new compliance mechanisms and so on. The underexplored statement that TCNs are only likely to be given to operators that are required to give effect to relevant authorisations on a "recurrent basis" (para 7.3) provides little clarity over who would be caught by this.

---

[41] *Privacy International v Investigatory Powers Tribunal* [2021] EWHC 27 (Admin) §48.
[42] ECtHR, *S and Marper v the United Kingdom* [GC], App No 30562/04, Judgment, 4 December 2008, §125.
[43] CJEU *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Ors* [GC], C-623/17, Judgment, 6 October 2020.

National Security Notices

For NSNs, the Code is explicitly open ended about their potential use [9.4-9.6]. The Code therefore offers no foreseeability and subjects operators to a regulatory regime in which anything can be enforced on them. An example given is "asking a telecommunications operator to refrain from doing something they might otherwise do" (para 9.6). That is excessively broad and could, in particular, be used to prevent security updates being sent.

For example, Section 252(3) IPA 2016 stipulates that an NSN may require an operator to:

- facilitate "anything done by an intelligence service" under any enactment other than the IPA 2016. This therefore includes measures taken under the Intelligence Services Act 1994, which has been used to authorise non-investigative forms of equipment interference[44]; or
- "provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively".

Insufficiency of existing limitations on NSNs

The limitations outlined in the Code in paras 9.7-9.9 do not help, because measures that undermine security and privacy will not always require a warrant or other authorisation, but as para 9.8 notes, could merely be a step in the process that would eventually require a warrant or authorisation, such as non-investigative equipment interference. Para 9.10 mandates that the SoS "must have particular regard to circumstances where a notice requires the taking of any steps that involve an interference with privacy".

However, it is unclear exactly what standard having "particular regard" means in this context and it should in any case be strengthened to ensuring compliance with everyone's rights (including, but not limited to, the right to privacy[45]). As a minimum, the wording from the Autumn 2016 version of the Code should be reinstated, under which a NSN could not be "used for the primary purpose of interfering with privacy, acquiring communications or data". Furthermore, the limitations in the Code do not address the wider concerns about undermining security identified above.

Necessity and proportionality

Paras 9.11-9.12 provide that the notices must be both necessary and proportionate. However, they do little to give confidence that NSNs can only be used lawfully: not least because they fail to mention the need to assess the impact on peoples' rights (compare with para 3.3 for Data Retention Notices, where the code at least realises that the proportionality test "involves balancing the extent of the interference with an individual's right to respect for their private life and, where relevant, with freedom of expression"). The mere existence of powers permitting

[44] See for example, *Privacy International v Investigatory Powers Tribunal* [2021] EWHC 27 (Admin).
[45] PI, 'Privacy Matters', https://privacyinternational.org/learning-resources/privacy-matters

the examination, use and storage of intercepted communications can constitute an interference with Article 8.[46]

Para 9.24 also states that a notice can only be given if it is necessary and proportionate. But again, it is a failed opportunity to explain more about what this means in practice.

Privileged communications and professional protections

Para 9.13 provides that it will "never be appropriate" to use an NSN without a warrant to obtain journalistic information or other "material of this nature". This fails to protect other professionals who are likely to hold sensitive information such as lawyers, doctors, therapists or politicians.

Removed example

The 2017 Code contained an example of what an NSN might look like and ought to consider in Annex A. This has been removed. Rather than removing this material, it should be built on to improve transparency and provide confidence that the regime will be operated in compliance with people's rights.

Notification Notices

The Code contains provision relating to the new regime for Notification Notices (NN). As with other forms of notice, PI is concerned that these could be used in ways that undermine the security of the internet and people's privacy. We consider that having to notify about changes in an operator's ability to provide communications data and/or content may have a chilling effect on the introduction of measures designed to protect online communications from hacking and intrusion.[47] These concerns are enhanced by the lack of Judicial Commissioner protection in the giving of NNs.

Our concerns are partly alleviated and partly exacerbated by para 14.12. Along with regulation 2(4)(b) of the draft SI, this provides that security patches (as defined by the NCSC) cannot be made the subject of a NN. That is a positive measure, which should also be applied to other notices in both the Code and relevant Regulations. Without it, the regime has uneven and unclear implementation and may be read to imply that TCNs and NSNs **can** be used to prevent security patches (which they should not). The current situation by which security updates are outside the scope of some (upstream) notices but not others is untenable. It creates uncertainty for operators and the public alike and fails to justify why it treats similar circumstances in materially different ways.

We also note the comments made by the Minister for Security during passage of the Investigatory Powers (Amendment) Act 2024 that the practice of combining

[46] See ECtHR, *Liberty and Others v United Kingdom*, , App No 58243/00, Judgment, 1 July 2008, §57.
[47] UNHRC, 'Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age', UN Doc A/HRC/51/17, 4 August 2022, https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf

notification notices with TCNs to prevent security updates was not "one that we have found or noticed in any way at all".[48] If that is the case, then this should be reflected in the law and the Code to provide certainty. The situation as is remains deeply problematic.

On the other hand, para 14.12 also states that "additional encryption on any aspect of its services … might constitute a relevant change" and therefore could be subject to a NN. For the reasons set out above and below, measures taken by the Government that interfere with and undermine encryption are not only deeply problematic but in conflict with international law.

The list of examples of relevant changes in para 14.11 is a useful addition and should be repeated for the other notices in the Code.

Oversight

Time periods

Para 13.33 of the Code states:

> *A renewal of a notice is required if two years has passed since the notice came into force, if it has been varied to include additional obligations or has been renewed. If a notice requires renewal, it must be renewed within the 30-day period ending with the day at the end of which the notice would otherwise cease to have effect. If a notice is not renewed within the period it will cease to have effect.*

A two-year period is too long to be the standard duration of a notice. This is because, as para 13.8 of the Code acknowledges, the "communications market is constantly evolving". A review of a notice should therefore be required if six months has passed since the notice came into force, considering that six months is also the default duration of many of the surveillance warrants under the IPA 2016.[49]

Statistics

A fundamental flaw with the notices regime is the lack of transparency over how the regime is operating, to whom notices have been given and what they are used for. The regime is extremely restrictive, including in preventing operators from sharing information about notices they have received, even when they are challenging them before the Investigatory Powers Tribunal (IPT).

Telecommunications operators are permitted to disclose statistical information about warrants in accordance with the Investigatory Powers (Disclosure of Statistical Information) Regulations 2018 (SI 2018/349). As a minimum, a comparable regime should be in place for notices, allowing operators to publish

[48] PBC Deb (Investigatory Powers (Amendment) Bill, 7 March 2024 (second sitting), col 56, https://hansard.parliament.uk/commons/2024-03-07/debates/68881a9b-e6d8-431a-b254-b4f226e79eb6/InvestigatoryPowers(Amendment)Bill(Lords)(SecondSitting)
[49] IPA 2016, ss 32(2)(b), 116(2)(b), 143(1), 162(1), 184(2)(b) and 213(2)(b).

aggregate statistical information about the notices they are subject to. Even better would be an obligation on the Secretary of State (or the Investigatory Powers Commissioner) to proactively publish information such as the number of notices approved, rejected, served, reviewed and renewed each year. This would add a vital degree of transparency and support the public's trust in the oversight regime without compromising the work of public bodies or the identity of any companies concerned.

Commissioner independence

In interpreting section 229 of the Act, para 15.3. of the Code states:

> *A Judicial Commissioner must, in particular, not jeopardise the success of an intelligence, security or law enforcement operation, compromise the safety or security of those involved, or unduly impede the operational effectiveness of an intelligence service, a police force, a government department or His Majesty's forces (see section 229(7)).*

However, the Act states that a "Judicial Commissioner must, in particular, ensure that the Commissioner does not" jeopardise the success of an operation etc. It is not clear whether this second appearance of the word Commissioner is referring to the Judicial Commissioner or the Investigatory Powers Commissioner. The way the Code is written does not help to resolve this matter. As it stands, the Code risks interfering with the independence and impartiality of the Commissioners by mis-stating what is in the Act.

For example, if a Judicial Commissioner does find that a notice sought by the Secretary of State is disproportionate and thus refuses to authorise it, their conduct could arguably fall within the Code's statement of the above prohibition of acting against national security interests or law enforcement, since any notice sought to be imposed would most likely seek to promote one of those objectives to a smaller or larger degree. However, that does not mean that the Investigatory Powers Commissioner is acting in such a way, nor that such action would not be justified by the Judicial Commissioner in appropriately carrying out their duties.

Review and appeal of notices

The Code is silent on the matter of the review and appeal of a notice beyond the oversight of the IPCO and ICO. If an operator were to continue to disagree with the legality of a notice, even after its approval by the Investigatory Powers Commissioner, the operator might be able to bring a challenge to the notice before the Investigatory Power Tribunal or the regular courts. Given the potential wide-reaching nature of notices, such a challenge may form an important, component of the oversight regime that gives room for consideration of the wider implications and harms of notices for all affected persons.

The Code would benefit from including guidance on such challenges, including how to navigate confidentially concerns while allowing as many third parties (including civil society, journalists and other operators) as possible to participate and so represent the full range of interests at play.

Overseas Dimensions

The ECHR and encryption

The lack of substantive and procedural safeguards in the UK notices regime means that it falls short of the standards required by the European Convention on Human Rights (ECHR).

Furthermore, in February 2024, the ECtHR reached an important decision in the case of *Podchasov v Russia*.[50] The case concerned a request by the Russian Federal Security Service (FSB) for Telegram to provide access to, and decryption keys for, the communications data and content of messages for six users. Ultimately, the case concerns a state's ability to require a telecommunications operator to assist its surveillance by undermining encryption. Just as notices may be used to do in the UK.

The Court found that tools that create backdoors into E2EE can violate people's right to private life and that a blanket requirement to decrypt encrypted communication is not necessary in a democratic society. The Court emphasised that technical or regulatory measures that undermine, break, or provide a 'backdoor' into encryption are problematic because, even if targeted at only particular users, they undermine the effectiveness of encryption for everyone. Decryption orders undermine the entire system of E2EE.

Allowing simply the possibility of a backdoor (or a requirement to maintain a capability) therefore allows for "routine, general and indiscriminate surveillance" (para 77, see also para 57). As a result, in *Podchasov*, the Court found that requiring an operator to weaken encryption for all users was not proportionate to the legitimate aims pursued (para 79).

This important conclusion highlights that E2EE helps protect rights and guard against abuses such as hacking:

> *In the digital age, technical solutions for securing and protecting the privacy of electronic communications, including measures for encryption, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression. Encryption, moreover, appears to help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information. This should be given due consideration when assessing measures which may weaken encryption.*[51]

Without E2EE, the security of the internet as a whole would no longer be assured, and "the protection afforded by Article 8 of the Convention would be

[50] ECtHR, *Podchasov v Russia*, App No 33696/19, Judgment, 13 February 2024.
[51] *Podchasov v Russia*, cited above, §76.

unacceptably weakened if the use of modern technologies in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such technologies against important private-life interests" (para 63). Finally, the Court recognised that there are alternative viable solutions for law-enforcement and security agencies (para 78).

This judgment demonstrates what careful consideration of the right to privacy and the need for online security demand with respect to powers that can be used to undermine E2EE. As it stands, the UK's notices regime fails to meet the standard set for adequate and effective safeguards and guarantees. At a minimum, the Code ought to be updated to reflect this important jurisprudence. Legislative change may also be necessary.

Finally, we draw the Government's attention to the fact that the ECtHR is not alone among international institutions recognising the central importance of E2EE to human rights, including the right to privacy. The following excerpts from UN bodies are particularly pertinent in demonstrating that weakening encryption does not meet the standards of international law and can fail the proportionality or necessity tests:

- The UN General Assembly has repeatedly stated that "technical solutions to secure and to protect the confidentiality of digital communications and transactions, including measures for strong encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association".[52] It has further urged governments to "refrain from interference with the use of technologies such as encryption and anonymity tools".[53] (December 2023)

- The UN Human Rights Council considers that "measures for encryption [...] are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association, and [...] States must promote such measures and refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking and restrictions on accessing and using encryption technology".[54] (October 2023)

- The UN High Commissioner for Human Rights stated in 2022 that "the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the

[52] UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/77/211, 15 December 2022, https://digitallibrary.un.org/record/3999709?v=pdf; UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213, 19 December 2023, https://digitallibrary.un.org/record/4032837?ln=en&v=pdf For past resolutions, see Privacy International, 'PI's Guide on International Law and Surveillance' (4th edn, September 2024), https://privacyinternational.org/report/5403/pis-guide-international-law-and-surveillance

[53] UN General Assembly Resolution on the Promotion and Protection of Human Right in the Context of Digital Technologies, UN Doc A/RES/78/213, 19 December 2023, §15, https://digitallibrary.un.org/record/4032837?ln=en&v=pdf

[54] UN Human Rights Council Resolution on the Right to privacy in the digital age, UN Doc A/HRC/RES/54/21, 12 October 2023, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F54%2F21

targeted individuals but the general population",[55] having noted in 2018 that weakening encryption "jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks. Such a widespread and indiscriminate impact is not compatible with the principle of proportionality".[56]

- The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has concluded that "the regulation of encryption often fails to meet freedom of expression standards in two leading respects. First, restrictions have generally not been shown to be necessary to meet a particular legitimate interest. This is especially the case given the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes. Second, they disproportionately impact the rights to freedom of opinion and expression enjoyed by targeted persons or the general population".[57]

- Lastly, the UN High Commissioner has found that "governments seeking to limit encryption have often failed to show that the restrictions they would impose are necessary to meet a particular legitimate interest, given the availability of various other tools and approaches that provide the information needed for specific law enforcement or other legitimate purposes".[58]

Conflict of laws

Paragraph 10.15. of the Code states:

> *When considering whether it is reasonably practicable for an operator outside the UK to take any steps in a country or territory outside the UK, regard must be given to any requirements or restrictions under the law of that country or that are relevant to the taking of those steps...*

More often than not, the Secretary of State will be confronted with such conflicts of law when considering the imposition of a notice upon an operator outside the UK. This is because many telecommunications operators have an international presence. As such, they potentially can be subject to conflicting legal obligations

[55] Report of the UN High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/51/17, 4 August 2022, §25, https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age
[56] Report of the UN High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, 3 August 2018, §20, https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high
[57] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on encryption, anonymity, and the human rights framework, UN Doc A/HRC/29/32, 22 May 2015, §39, https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework
[58] Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/51/17, 4 August 2022, §24, https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

imposed by multiple legal orders – from the US and the UK, to Russia and China and the European Union.[59] How those conflicts should be resolved remains the subject of significant ongoing discussion.[60] For example, the conduct sought to be achieved through the imposition of a notice might be prohibited or might require prior independent judicial authorisation in certain jurisdictions.

At the same time, as a result of the proliferation of incidents threatening the integrity of consumer data and the security of connected devices, several jurisdictions have in the last few years adopted cybersecurity legislation that imposes strict obligations upon operators to prevent, address and report any conduct that could potentially pose a threat to the security or privacy of their products and services.[61]

Let us consider the following scenario:

The Secretary of State considers imposing a Technical Capability Notice upon an EU based telecommunications operator. The latter is a smartphone manufacturer that provides both hardware and software for about 100 million users in the EU. The operator's annual global revenue is about EUR 120 million. The proposed TCN would require the operator to refrain from patching a recently discovered software vulnerability in the OS of its smartphones for a certain period of time.

However, as they offer services to EU consumers too, the operator is subject to the Cyber Resilience Act (CRA), which requires the operator to, amongst others, immediately address and remediate any software vulnerabilities as well as to report any actively exploited vulnerabilities. Under the CRA, failure to comply with the above requirements would result in an administrative fine of EUR 15 million or up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

In the present scenario, the operator is essentially confronted with a regulatory conflict. On the one hand, if they choose to comply with the TCN, they risk being subject to harsh administrative fines, which might be taken on by the UK Government, and irreparable reputational harm across a vast market. On the other hand, if they choose to comply with their obligations under EU law, then the Secretary of State might bring civil proceedings against them. Eventually, operators with a strong EU presence that are the potential recipients of notices might likely carry out a cost benefit analysis and, in light of the potential risks, decide to abandon their UK presence or cease to offer services in the UK.

[59] See further our response to the 2023 consultation on the notices regime, https://privacyinternational.org/advocacy/5088/pi-response-uk-government-consultation-technical-capabilities-notices

[60] See, for example, IJPN, 'Internet & Jurisdiction Global Status Report 2019', 27 November 2019, https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report; Pedro de Miguel Asensio, *Conflict of Laws and the Internet* (Edward Elgar Publishing 2020).

[61] For instance, in October 2024, the EU adopted the Cyber Resilience Act (Regulation 2024/2847), which introduces EU-wide cybersecurity requirements for the design, development, production and making available on the market of hardware and software products, while imposing strict security handling and reporting obligations upon device manufacturers and software vendors. See particularly Chapter II and Annex I of the Act.

PI submits that any potential conflict of law, such as those described in the scenario above, should be resolved in favour of permitting operators to not comply with the requirements of a notice if they are prevented from doing so by a requirement under the law of the state they are based in. This approach does not only ensure that the UK complies with its obligations under international human rights law, but it also reduces the significant financial risk.[62]

EU adequacy

On 28 June 2021, the European Commission adopted two adequacy decisions for the United Kingdom under the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).[63] The former is based on Article 45(1) GDPR which provides that transfers of personal data between the Union and a third country may take place where the Commission has decided that the third country "ensures an adequate level of protection".

As the Court of Justice of the EU (CJEU) has held, the level of protection required by Article 45 GDPR must be read in light of the provisions of the Charter of Fundamental Rights of the EU (CFREU).[64] Article 52(3) of the Charter stipulates that the rights guaranteed in the Charter correspond to the rights guaranteed by the European Convention on Human Rights and the CJEU has held that account must "be taken of the corresponding rights of the ECHR for the purpose of interpreting the Charter, as the minimum threshold of protection".[65] In issuing the adequacy decisions of 28 June 2021, the European Commission relied heavily on the existence of safeguards under UK law. It underlined:

> *In particular, the collection of data by intelligence authorities is, in principle, subject to prior authorisation by an independent judicial body. Any measure needs to be necessary and proportionate to what it intends to achieve. Any person who believes they have been the subject of unlawful surveillance may bring an action before the Investigatory Powers Tribunal. The UK is also subject to the jurisdiction of the European Court of Human Rights and it must adhere to the European Convention of Human Rights as well as to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which is the only binding international treaty in the area of data protection. These international commitments are an essential elements (sic) of the legal framework assessed in the two adequacy decisions.*[66]

Further, we note that the European Data Protection Board (EDPB) has expressed concerns with regard to the existence of "avenues for the exercise of rights for the

[62] For example, in 2022 alone, the EU regulatory fines against big tech companies exceeded USD 3 billion.
[63] Commission Implementing Regulation 2021/1772 and Commission Implementing Decision 2021/1773, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents
[64] See CJEU, *Facebook Ireland and Schrems*, C-311/18, Judgment, 16 July 2020, §§99-101.
[65] CJEU, *La Quadrature du Net and others,* joined cases C-511/18, C-512/18 and C-520/18, Judgment, 6 October 2020, §124.
[66] European Commission, Data protection: Commission adopts adequacy decisions for the UK, Brussels, 28 June 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

data subjects concerned, and possible redress avenues offered to them in the context of equipment interference operations, especially when they take place in the context of urgency leading to a derogation to the double-lock procedure".[67] Similar criticisms were also voiced by the European Parliament in its resolution of 21 May 2021.[68]

For the reasons discussed above, we submit that, in its current form, the Code will likely raise significant compatibility issues with international law which could accordingly threaten the UK's adherence to its obligations under international human rights law. It could also put both the current as well as any future EU adequacy decisions in jeopardy.

We therefore urge the UK Government to use this opportunity to update its framework to account for these developments, to prevent non-compliance with international law and standards, and to maintain its position on the global stage.

Recommendations

The Government must rebalance and stabilise the notices regime by putting in place clear substantive restrictions and limitations (in both law and the Code) as to what notices cannot be used for. Measures must also be taken to reflect recent developments in international law and to improve the oversight and transparency of the regime.

Privacy International recommends that:

8. When providing guidance about general obligations or matters that apply to more than one type of notice (such as under section 2 or section 255 or in relation to necessity and proportionality), the Code should either use the same language and content across the different notices, or explain why a different approach is justified for different types of notices.

9. The Code should provide examples of the concrete implications of the general duties found in section 2.

10. The paragraphs of the Code that refer to section 255 should be amended to prevent overbalancing the consideration given to benefits, especially where those benefits are speculative or projected. The Code should also explicitly recognise (for both NCNs and TCNs) that the likely number of users includes people from outside the UK and consider the wider costs an imposition of a notice might have for an operator and its users. The Secretary of State should also consider representations made by relevant regulators.

[67] EDPB, 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom', 13 April 2021, https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf, §166.
[68] European Parliament, Resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom, 2021/2594(RSP), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0262

11. The Code and relevant regulations should be amended to prohibit TCNs and NSNs being used to undermine encryption (whether directly or indirectly), not least to ensure compliance with the ECHR.

12. The Code and relevant regulations should be amended to prohibit TCNs and NSNs being used to prevent security updates, following the lead of the new regulations and code on notification notices and so preventing uneven, unclear and incoherent implementation of the notices regime. This is also necessary to accord with comments made by the Minister of Security.

13. The Code should be amended to state that NSNs must comply with people's rights, including to privacy, and that their primary purpose cannot be to interfere with privacy, or to acquire communications or data. Notices must not be used to circumvent a lack of statutory authorisations to obtain data and interfere with privacy protections.

14. The Code should protect professionals other than journalists who are likely to hold sensitive information.

15. The Code should provide greater detail about how the requirements for necessity and proportionality operate. As a minimum, the Code should be elaborated on to say:

    a. Interception of communications and associated data will always entail an interference with a person's rights under the ECHR;
    b. Full and thorough consideration must be given as to whether other less invasive techniques have been exhausted;
    c. What considerations are relevant to assessment of the intrusiveness of a measure.

16. The Code should explain what it means for requirements to be 'reasonably practicable', in particular with reference to the capability to remove encryption and the need to avoid blanket and indiscriminate measures.

17. The Code should provide more concrete examples as to what notices can be used for (as is done for notification notices).

18. Notices should be reviewed six months (rather than two years) after they come into force, varied or renewed. If a notice is not reviewed within a 30-day period, then it should cease to have effect.

19. A mechanism for general statistical information about notices being published regularly should be established.

20. The Code should include guidance on how third parties (including civil society, journalists and other operators) can participate in challenges to notices before the IPT while maintaining confidentiality.

21. The Code (and legal framework) should be brought into line with the UK's obligations under the ECHR and best practice as recommended by UN institutions.

22. Operators should not be obliged to comply with a notice if doing so would cause them to breach a legal obligation under the law of the state in which they are based.

23. The UK should ensure that the code does not jeopardise adequacy under EU data protection law.

IV. Ongoing Concerns Beyond the Current Updates to the Codes

While not explicitly at issue in this consultation, PI has ongoing concerns about two categories of investigative powers covered by the codes: thematic warrants and the bulk powers, including bulk retention of communications data. These concerns provide context to our more specific recommendations regarding the amendments being consulted upon.

Thematic Warrants

As we have raised often in the past[69], thematic warrants grant the Government the power to conduct surveillance of a group or category of people without requiring each target of the surveillance to be identified in the warrant. While contained within the "targeted" surveillance provisions of the IPA focused on interception and equipment interference, thematic warrants have the potential to be bulk surveillance in disguise, with all its attendant risks and human rights concerns. The use of thematic warrants upends a long tradition in the UK of prohibiting 'general warrants', which the High Court recently reiterated. [70]

These thematic warrants, once granted for ill-defined categories or groups of people (or equipment), delegate to the police or intelligence agencies the decision as to whose privacy will be interfered with. This increases the risk of arbitrary action and undermines the implementation of effective authorisation and oversight. The current codes have taken some steps toward trying to cabin this potential for arbitrariness and abuse by providing guidance on the level of specificity required in thematic warrants and scenarios that require a bulk warrant instead of a thematic warrant.[71] But the sample warrants described in these sections are still extremely vague and broad. For instance, Example 1 in paragraph 5.39 of the Draft Equipment Interference Code of Practice suggests a thematic warrant may be appropriate to authorise the interference with the equipment of "a number of unidentified criminal associates are planning to imminently commit a serious criminal offence" where the people and equipment who are eventually interfered with will never be specifically identified to the authorising authority. As with the notices, thematic warrants need clearly delineated limitations, not just illustrative examples which in themselves seem to place few boundaries on these overly broad powers. Otherwise, too much decision-making power is delegated, leading to the potential for arbitrariness and abuse. Post hoc oversight, such as that exercised by the Investigatory Powers Commissioner, may help remedy harms but is not sufficient to prevent them.

---

[69] See, e.g., Privacy International's written evidence submitted to the Joint Committee on the Investigatory Powers Bill, https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26371.html; see also, PI, 'Destroying Democracy Under the Cloak of Defending It', 7 March 2026, https://medium.com/privacy-international/destroying-democracy-under-the-cloak-of-defending-it-4a46727ea272

[70] *Privacy International v Investigatory Powers Tribunal and ors* [2021] EWHC 27 (Admin); see also, PI, 'Victory at the High Court against the government's use of 'general warrants', 8 January 2021, https://www.privacyinternational.org/news-analysis/4359/victory-high-court-against-governments-use-general-warrants

[71] DRAFT Equipment Interference Code of Practice, §§5.17-5.22, 5.37-5.39.

Bulk Powers

Privacy International has brought several legal challenges over the years against the disproportionate use of surveillance powers by UK authorities, such as the bulk interception of communications[72], bulk hacking[73], and the bulk retention and collection communications data[74] from telecommunications companies. The UK has been found in violation of human rights obligation in every instance. This demonstrates how difficult it is to ensure these powers are deployed in accordance with fundamental human rights and rule of law. Among others, the Investigatory Powers Tribunal (IPT), the judicial body responsible for monitoring UK intelligence and security agencies, has found that all three agencies – Government Communications Headquarters (GCHQ), Security Service (MI5) and Secret Intelligence Service (SIS) – were unlawfully holding data relating to Privacy International and the Security Service had accessed it.[75] While on 30 January 2023, the IPT found that MI5 unlawfully retained huge amounts of personal data between 2014 and 2019.[76]

These submissions are without prejudice to the arguments we have brought forward in previous legal challenges and advocacy submissions. We continue to maintain that the United Kingdom should revise its current legal regime to ensure it is compliant with its human rights law obligations.

We submit that bulk surveillance powers that involve the acquisition, processing, generation, analysis, use, retention or storage of information about large numbers of people, without any regard to whether they are suspected of wrongdoing is incompatible with human rights law. Bulk surveillance powers subject a population or significant component thereof to indiscriminate monitoring, involving a systematic interference with people's right to privacy and all the rights that privacy enables, including freedoms of expression and assembly.

Therefore, as such, bulk surveillance threatens the essence of the right to privacy and fails to comply with the principles of necessity and proportionality putting at risk core democratic principles and the rule of law. Bulk surveillance is neither strictly necessary nor proportionate in a democratic society. There are more often than not less invasive alternatives to bulk surveillance powers that could be deployed.

[72] PI, '10 Human rights orgs v the United Kingdom', https://privacyinternational.org/legal-action/10-human-rights-organisations-v-united-kingdom
[73] PI, 'The Queen on the application of Privacy International v Investigatory Powers Tribunal (UK General Hacking Warrants)', https://privacyinternational.org/legal-action/queen-application-privacy-international-v-investigatory-powers-tribunal-uk-general
[74] CJEU, *Privacy International v the United Kingdom*, C-623/17, Judgment, 6 October 2020, https://privacyinternational.org/legal-action/cjeu-bulk-challenge; see also PI, 'Watson/Tele2 case', CJEU, https://privacyinternational.org/taxonomy/term/410
[75] PI, 'Bulk Personal Datasets & Bulk Communications Data challenge', https://privacyinternational.org/legal-action/bulk-personal-datasets-bulk-communications-data-challenge
[76] PI, 'MI5 ungoverned spaces challenge', https://privacyinternational.org/legal-action/mi5-ungoverned-spaces-challenge

Recommendations recap

Annex A

1. Annex A must make clear what categories of data will not be gathered as part of a Low Privacy BPD.

2. While we raised the absence of a discrete legal basis and Code of Practice for the use of BPDs for machine learning purposes above, at a minimum we consider that Annex A must confirm whether personal data contained in a Low Privacy BPD will be used to train machine learning models. It should also provide confirmation as regards what categories of data will be used for such purposes; how sensitive information that would otherwise not fit within a Low Privacy BPD would be erased or removed from the dataset once deployed for training purposes; and how proportionality and necessity can be assessed (including consideration of when it would not be appropriate to use datasets for training purposes).

3. If the above information is not provided, we consider that personal data contained within Low Privacy BPDs should not be used to train and develop machine learning models.

Annex B

4. Where access to a 3PD is likely to involve the intelligence services examining personal data, the authorisation process should include an assessment of the lawfulness of the information to be accessed, in particular its compliance with data protection legislation. This assessment should be carried out by a legal adviser within the intelligence services.

5. Where personal data is likely to have been processed unlawfully by the third-party it should not be accessed or examined by the intelligence services.

6. Annex B should set out the conditions under which access to a 3PD will be granted, how the intelligence services will ensure that data is not copied over to their own systems during and following examination, and how access will be terminated following the refusal, expiry, and/or non-renewal of a 3PD warrant.

Annex C

7. Annex C should clarify whether Low Privacy BPDs would be used to train automated systems that select data within part 7 BPDs for examination by the intelligence services.

Annex H

8. When providing guidance about general obligations or matters that apply to more than one type of notice (such as under section 2 or section 255 or in relation to necessity and proportionality), the Code should either use the same language and content across the different notices, or explain why a different approach is justified for different types of notices.

9. The Code should provide examples of the concrete implications of the general duties found in section 2.

10. The paragraphs of the Code that refer to section 255 should be amended to prevent overbalancing the consideration given to benefits, especially where those benefits are speculative or projected. The Code should also explicitly recognise (for both NCNs and TCNs) that the likely number of users includes people from outside the UK and consider the wider costs an imposition of a notice might have for an operator and its users. The Secretary of State should also consider representations made by relevant regulators.

11. The Code and relevant regulations should be amended to prohibit TCNs and NSNs being used to undermine encryption (whether directly or indirectly), not least to ensure compliance with the ECHR.

12. The Code and relevant regulations should be amended to prohibit TCNs and NSNs being used to prevent security updates, following the lead of the new regulations and code on notification notices and so preventing uneven, unclear and incoherent implementation of the notices regime. This is also necessary to accord with comments made by the Minister of Security.

13. The Code should be amended to state that NSNs must comply with people's rights, including to privacy, and that their primary purpose cannot be to interfere with privacy, or to acquire communications or data. Notices must not be used to circumvent a lack of statutory authorisations to obtain data and interfere with privacy protections.

14. The Code should protect professionals other than journalists who are likely to hold sensitive information.

15. The Code should provide greater detail about how the requirements for necessity and proportionality operate. As a minimum, the Code should be elaborated on to say:

    a. Interception of communications and associated data will always entail an interference with a person's rights under the ECHR;
    b. Full and thorough consideration must be given as to whether other less invasive techniques have been exhausted;
    c. What considerations are relevant to assessment of the intrusiveness of a measure.

16. The Code should explain what it means for requirements to be 'reasonably practicable', in particular with reference to the capability to remove encryption and the need to avoid blanket and indiscriminate measures.

17. The Code should provide more concrete examples as to what notices can be used for (as is done for notification notices).

18. Notices should be reviewed six months (rather than two years) after they come into force, varied or renewed. If a notice is not reviewed within a 30-day period, then it should cease to have effect.

19. A mechanism for general statistical information about notices being published regularly should be established.

20. The Code should include guidance on how third parties (including civil society, journalists and other operators) can participate in challenges to notices before the IPT while maintaining confidentiality.

21. The Code (and legal framework) should be brought into line with the UK's obligations under the ECHR and best practice as recommended by UN institutions.

22. Operators should not be obliged to comply with a notice if doing so would cause them to breach a legal obligation under the law of the state in which they are based.

23. The UK should ensure that the code does not jeopardise adequacy under EU data protection law.