

Joanna Cherry KC MP
Joint Committee on Human Rights
Houses of Parliament
London
SW1A 0AA

By email only

19 March 2024

Dear Joanna,

Investigatory Powers (Amendment) Bill

I am grateful for the Committee's scrutiny of the Investigatory Powers (Amendment) Bill ("the Bill") and for your letter of 6 March setting out the Committee's views on the Bill. As you are aware, the Government's clear view is that the Bill is compatible with the European Convention on Human Rights (ECHR)¹. I am, of course, more than happy to provide clarification on the points raised in your letter.

Notification notices – security patches

The Committee have asked for reassurances about "security patches". We would never stop an essential security patch to a system and cannot foresee a circumstance in which a security patch would have such sweeping effect on lawful access capabilities. As defined by the National Cyber Security Centre- "*A security patch fixes a defect in installed software and leaves the intended functionality of the software unchanged*". Any security update, patch or fix that meets this definition will be out of scope.

Given the technical nature of a security patch and the fast-changing nature of technological development, it is more practical to specify this within secondary legislation rather than on the face of the Bill, which will allow further context regarding the definition. My department published a policy statement in December 2023² setting out further detail regarding the intention of the regulations that will implement the provisions, including relevant changes operators will be required to notify the Secretary of State of. These changes relate specifically to the protection of lawful access capabilities, and the statement specifies that security patches are not considered a relevant change. Additional guidance will be provided in the regulations or related Codes of Practice, as appropriate. The Regulations and codes of practice will both be subject to full public consultation and Parliamentary scrutiny under the affirmative procedure.

¹ <https://bills.parliament.uk/publications/52927/documents/3987>

² <https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-policy-statement>

Notification notices – Judicial Commissioner review

Your letter asks the government to consider requiring Judicial Commissioner (JC) approval for the issuing of a notification notice. Notification notices are intended to be a lighter-touch notice requiring a telecommunications operator to simply notify the Secretary of State of a proposed change, with no actual interference with user privacy or in the proposed change itself. This is inherently different from the other types of notices, where there is the potential for warranted interference with user privacy. Therefore the double lock is appropriate to ensure the necessity and proportionality considerations are subject to judicial oversight.

The Bill has sought to replicate in the notification notices many of the other safeguards already in place for the other notices. The Secretary of State is required to consider necessity and proportionality, and a series of further factors must be considered before the notice is given (laid out in clause 21(2), sections 258A(5) and (6)). Therefore the approach in the Bill is the result of a careful consideration of what notification notices are intended to achieve and both their similarities and differences from existing notices regimes.

Notices review

During Committee Stage in the House of Lords, the Government tabled amendments to the Bill which introduced a new regulation-making power to enable the Secretary of State to specify in regulations the length of time the Secretary of State can take to reach a decision on the review of a notice upon receipt of the report by the JC and the Technical Advisory Board (TAB), and the overall length of time that a review can take. The TAB's membership includes representatives from the telecommunications industry, government/public authorities, and independent members including an independent chair.

Specifying timelines will require an amendment to the existing regulations concerning the review of notices. The government committed to holding a full public consultation before the amendment of those regulations and the laying of new regulations relating to Clause 21, which provides for the introduction of the notification notices. It is important that this consultation informs the decision on the most appropriate length of time for a review.

I note the Committee's suggestion to amend the process for a review of a notice to improve the independence of appeals. Whilst it is correct that the review is decided by the same Secretary of State who gave the original notice, there are independent safeguards already built into that process. The process requires the Secretary of State to consult the TAB, who must consider the technical requirements and financial consequences of the notice, and an independent JC (i.e. a different Commissioner to the one who approved the original notice) who must consider whether the notice, so far as referred, is proportionate.

Before reaching their conclusions, the Board and the Commissioner must give the operator and the Secretary of State an opportunity to provide evidence or make representations to them. After considering reports from the TAB and the JC, the Secretary of State may decide to vary, revoke or confirm the effect of the notice. Where the Secretary of State decides to confirm or vary the notice, the Investigatory Powers Commissioner must approve the decision. This means the Secretary of State cannot unilaterally give a notice following a review and there will always be independent judicial oversight within the process.

I hope that this provides reassurance to the Committee on that point.

Low/No Bulk Personal Datasets – scope of Part 7A

The Committee has asked for greater clarity on what will be in scope of new Part 7A. The question of whether a dataset meets the low or no reasonable expectation of privacy test will be assessed on a case-by-case basis, having regard to all the circumstances, and in particular the factors set out in the Bill. It is a nuanced assessment that is not capable of being reduced to an arbitrary list.

The test set out under section 226A is framed around the concept of “reasonable expectation of privacy” because this is the jurisprudential touchstone for the engagement of the right to a private and family life in Article 8 of the ECHR. The Bill lists a number of factors that are germane to the exercise of considering low or no reasonable expectation of privacy, which are drawn from existing caselaw and are drafted in such a way as to ensure that future developments in the jurisprudence can be accommodated. This is because the law concerning the reasonable expectation of privacy is continually developing, and the provision is intended to be sufficiently flexible to accommodate future changes.

The types of data that may fall within the scope of the Part 7A regime include, but are not limited to: news articles, academic papers, public and official records, online encyclopedias, audiobooks and podcasts, content derived from online video sharing platforms, publicly available information about public bodies, corporate registry and trade data, and internet infrastructure and operating data. Paragraphs 4.14 to 4.20 of the draft Part 7A code of practice³ set out further detail and examples of the types of datasets that would meet the test at 226A.

In respect of how leaked data will be approached, there is a helpful example in the independent review by Lord Anderson of Ipswich KC⁴: the Enron corpus. This is a large dataset of emails that came into the public domain following the investigation into the collapse of the Enron Corporation. Although this dataset was not hacked per se, it was initially sensitive. The dataset has been available in various forms for almost 20 years and is widely used in data science. It is right that such datasets could be in scope of the new regime where the test is met.

It is more appropriate that this level of detail is set out in the code of practice rather than on the face of the legislation. The IPA codes are statutory and due regard must be had to them when exercising the powers. The new code of practice for Part 7A must be subject to a public consultation before it is brought forward and will then be brought into force in accordance with an affirmative statutory instrument, providing the opportunity for public and parliamentary scrutiny.

Low/No Bulk Personal Datasets – sensitive datasets

In terms of sensitive data being out of scope of Part 7A, as the factors set out in section 226A make clear, particular regard must be had to the nature of the data in a bulk personal dataset (BPD) before concluding that it falls within Part 7A. A BPD that does not fall within Part 7A may then be considered for authorisation under the existing Part 7 regime.

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.

3

<https://assets.publishing.service.gov.uk/media/6570928d809bc3000d30819c/20231130+FINAL+DRAFT+Part+7A+code+of+practice+CLEAN.docx>

⁴ [Independent review of the Investigatory Powers Act 2016 - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/657092/Independent_review_of_the_Investigatory_Powers_Act_2016.pdf)

In relation to what would happen if an officer examining a low/no BPD discovered that it contained more sensitive data, Section 226D sets out the process for this. The Head of the intelligence service must ensure that anything in the process of being done in relation to that part of the dataset is stopped as soon as is reasonably practicable. The intelligence service must then treat that part of the dataset as if the relevant authorisation had been cancelled. The relevant data must be removed from the dataset and it will then either be deleted, or a Part 7 warrant may be sought in respect of it. This process has been clarified in the draft code of practice at paragraphs 4.22 – 4.27.

Low/no bulk personal datasets – time period for renewals

The Committee suggested that the three month time limit permitted under Clause 226CD should be reduced to three days. The intention behind the three-month time limit is to prevent a “cliff edge” scenario which would risk the interruption of operational activity and an overwhelming resource burden on both the intelligence service itself and on the Investigatory Powers Commissioner’s Office (IPCO).

In the event that a category authorisation is cancelled or is not renewed, during the subsequent three-month period the intelligence service must decide what it is to do in respect of the continued authorisation of what may be a considerable number of datasets that were individually authorised in reliance on the category authorisation. The period allows time for an orderly decision-making process and the appropriate sequencing of any subsequent applications. Were this time limit to be reduced in line with the Committee’s suggestions, it would mean that the intelligence services would likely need to identify and decommission operational systems and capabilities developed in reliance on certain datasets, which would not be reasonably practicable to do within three days, leading to interruption of operational activity.

Child Rights Analysis

You asked about child rights and use of investigatory powers. There are robust safeguards built into the IPA that apply to the use of all investigatory powers by public authorities. It must be borne in mind that investigatory powers under the IPA are authorised on a case-by-case basis where it is necessary for specific statutory grounds and the proposed activity is a proportionate response to what is sought to be achieved. The vulnerability of children and lack of control over their own data should therefore be factors in any proportionality assessment where it is relevant to a particular application. It is equally worth highlighting that section 2 of the IPA makes clear that those exercising powers must have regard to certain considerations, including whether the same effect could reasonably be achieved by less intrusive means.

Third Party Bulk Personal Datasets (3PDs)

Third parties obtain and store data on their systems in accordance with their routine business objectives and legal requirements. As the intelligence services are not the data controller of these datasets, they are not responsible for how the data is obtained by the third parties and Part 7B does not amend any legal requirements on the third party. Third parties are subject to the usual rules and requirements that apply to the collection and retention of data.

The examination of a 3PD by an intelligence service requires a double locked warrant, meaning the decision to authorise examination of a 3PD will need to be approved by both the Secretary of State and an independent JC, and the intelligence service will need to provide a description of the 3PD as part of the warrant application. The Secretary of State may not issue the warrant unless they consider doing so is necessary and proportionate, and that there are satisfactory arrangements made by the intelligence service for examining the dataset.

Internet Connection Records

As with all investigatory powers, the case for requesting Internet Connection Records (ICR) data must be necessary and proportionate, and intelligence-led. New condition D enables a request for details to identify individual(s) who have used one or more specified internet services in a specified time frame to allow for target detection.

The data returned is very likely to be limited to a list of IP addresses or the individuals' names and addresses. Condition D does not allow the collection of information about wider internet activity for those individuals. The use of ICRs for target detection could revolutionise the ability of investigators to prosecute serious criminals, including those engaged in child sexual abuse and exploitation and those who would seek to undermine our National Security.

The new condition will also be subject to robust safeguards including limiting the statutory purposes available, stringent necessity and proportionality requirements, and independent oversight including regular inspections by IPCO. Applications solely for serious crime purposes which are not urgent will also be subject to prior independent approval by IPCO, in line with the wider approach to communications data acquisition under the existing Act.

IPCO carries out regular inspections – at a time and frequency of their choosing - and can request sight of all authorisations and associated documents that they wish to see. This will ensure compliance with high standards and safeguards. Any concerns will be raised with the relevant organisation and must be addressed, and these issues can be highlighted in the IPC's Annual Report in which the IPC may draw out any errors as he deems appropriate.

The IPA has an existing error reporting regime, which requires public authorities, telecommunications operators and postal operators to report "relevant errors" of which they are aware to the IPC and his office. IPCO will then review any reported relevant error and may recommend further mitigatory action as appropriate. The IPC is also able to inform an affected person if they have been the subject of a serious error. Individuals are able to make complaints to the Investigatory Powers Tribunal if they think they have been the subject of any unlawful use of investigatory powers.

I hope that the detail provided in my response has provided reassurance to the Committee on the issues raised. I remain grateful for your consideration of the Bill and the constructive and thoughtful engagement of the Committee staff.

A copy of this letter goes to the Chair of the Home Affairs Select Committee.

Yours,

A handwritten signature in blue ink, appearing to read 'Tom Tugendhat', is written over a light blue horizontal line.

Rt Hon Tom Tugendhat MBE VR MP
Security Minister