March 4, 2024

House of Commons Public Bill Committee
scrutiny@parliament.uk

Written Evidence Submission on the Investigatory Powers (Amendment) Bill

On behalf of the Center for Data Innovation, we are pleased to submit this response to the House of Commons Public Bill Committee's (PBC) call for evidence in respect to the Investigatory Powers (Amendment) (IPA) bill.

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

EXECUTIVE SUMMARY

In this submission, we make the following points:

1. The IPA bill should clearly define what type of data falls within "low or no expectation of privacy";
2. The PBC should revise the proposed measures for the notice regime that in their current state are overreaching, reduce UK competitiveness, and favour national security at the expense of consumer protection; and
3. The IPA should maintain the requirement for pre-requisite knowledge in the use of Internet Connection Records for the detection of high-impact offenders.

1. THE IPA BILL SHOULD CLEARLY DEFINE WHAT TYPE OF DATA FALLS WITHIN "LOW OR NO EXPECTATION OF PRIVACY"

1.1. The current proposals seek to amend Part 7 of the Investigatory Powers Act 2016 ("the Act") to introduce a new category of Bulk Personal Datasets (BPDs) in respect of which there is a low or no expectation of privacy ("LNEP" data), such that any data falling within this category is subject to a lower threshold of safeguards.

1.2. We support the use of already publicly available data to develop information and technology services, such as the training of machine learning (ML) models to maximise the benefits of digital transformation whilst protecting national security.[1] However, we are concerned that the introduction of a new category of data outside of the Data Protection Act (DPA) may infringe upon individual privacy rights if left undefined and without proper scrutiny as to its necessity and proportionality.

1.3. In its current state, it is unclear exactly what type of data would be classed as LNEP data. We are concerned that such data may include data publicly available but that, nonetheless, if processed, would be considered highly intrusive by data subjects.

1.4. Given that this category would be subject to a less onerous set of safeguards, a clear definition coupled with objective examples should be included in the IPA or alternatively required of the Secretary of State to outline in accompanying guidance to prevent subjective assumptions from security services.

1.5. At the very least, Judicial Commissioners (JCs) should be empowered to evaluate the necessity and proportionality of a warrant and the consideration of the subject data of the warrant falling within this definition of LNEP data. This consideration should also be subject to review by the Investigatory Powers Commissioner's Office (IPCO).

1.6. Similarly, we would also welcome greater clarity on what distinct safeguards would apply to LNEP data, either in the IPA itself or with accompanying guidance.

1.7. Greater clarity for the safeguards and the definition of LNEP data would go far to better inform UK citizens of what data is subject to this type of lawful access and the controls in place to limit infringements.

[1] Investigatory Powers (Amendment) Bill [HL] Explanatory Notes, page 10.

2. THE PBC SHOULD REVISE THE PROPOSED MEASURES FOR THE NOTICE REGIME THAT IN THEIR CURRENT STATE ARE OVERREACHING, REDUCE UK COMPETITIVENESS, AND FAVOUR NATIONAL SECURITY AT THE EXPENSE OF CONSUMER PROTECTION

2.1. The proposed amendments to Part 4 and Part 9 of the Act would introduce a new "maintaining the status quo" obligation during a notice review period; expand the definition of "telecommunications operator"; require telecommunications operators to inform the Secretary of State of any proposed changes to their services that would affect the lawful access capabilities of state security services; introduce a statutory footing for the Investigatory Powers Commissioner (IPC) to oversee the notice renewal process; and allow the Secretary of State to set the timeline for the overall review period of a notice.

2.2. We believe that such amendments, if enacted, would significantly weaken the UK's position as a global technology hub, and that the pursuit of such a protectionist regime unjustly favours interests of national security over consumer protection.

2.3. Firstly, introducing a status quo requirement during a notice review period would have the effect of preventing telecommunications operators from executing security updates or feature upgrades. This would impact the speed at which UK consumers and businesses can use new technology by slowing down development and introducing unnecessary and potentially disproportionate red tape for the benefit of state security services.

2.4. Under the revised regime, whilst there is no blocking power to outrightly prevent operators from changing their services once a notice is given, the requirement to maintain the status quo would in effect achieve the same outcome, requiring operators to ensure that, where a notice is under review, lawful access to data is maintained. Coupled with the new proposal to allow the Secretary of State to set the timeline for a review (dealt with below), operators would be required to keep their services as they are for a potentially significant period of time, which would have a detrimental impact on the overall provision of services to the UK.

2.5. For example, services such as messaging apps, dating apps, gaming platforms and more that wish to implement or update their end-to-end encryption for user-to-user communications would be subject to these requirements. Operators may find themselves unable to implement best practices, leaving their users at risk of data breaches from malicious actors, including foreign adversaries.

2.6. The proposed amendment therefore not only undermines consumer protection, but also works against national security interests by making it harder for operators to address risks to UK citizens' data. We therefore urge the PBC to reconsider the inclusion of the requirement to maintain the status quo.

2.7. Secondly, the expansion of the definition of "telecommunications operator" to include businesses operating, but not based, in the UK, cuts down on the global access the UK has to technology.

2.8. This obligation would reduce the UK's competitiveness as a global tech hub, with Meta and Apple stating clearly that they would not compromise user privacy and security, the latter of which stated the near certainty of pulling services in the event of the IPA moving forward in its current state.[2] We therefore urge the PBC to reconsider the applicability of the definition to operators servicing the UK from abroad who, as a result, would be reduced to offering a limited service specific to the UK.

2.9. Thirdly, the requirement to inform the Secretary of State of proposed changes would require businesses to anticipate and guess which of their services and products may affect the lawful access requirements of security services.

2.10. This requirement is overly burdensome on businesses by placing the onus on them to anticipate government access requirements, resulting in a high likelihood of false negatives (operators informing the Secretary of State of a change that the Secretary of State deems fine) and false positives (operators failing to inform the Secretary of State of a change that the Secretary of State deems problematic). In either event, both would require extensive resource to identify which changes may fall under the IPA and expose operators to possible penalties if they get the latter wrong.

2.11. Such an environment is unsustainable in an industry with ubiquitous fast-changing technology that could be delayed in the instance of a false negative, and completely disrupted in the instance of a false positive.

2.12. To resolve this, the Secretary of State should be required to set out a pre-determined list that highlights the categories of change requiring notification to the Secretary of State, such as changes affecting specific lawful access by state actors.

2.13. Finally, whilst we support the introduction of a statutory role for the IPC to oversee the notice renewal process, we do not agree with the additional power of the Secretary of State to unilaterally determine the timeline of the overall review period for a notice. This power should be approached with the same level of scrutiny as the authorisation process of warrants for BPDs, with a "double lock" authorisation provided by an independent JC

[2] "UK to work 'constructively' with Meta over encryption and online safety", Sarah Young et al, Reuters, 20 September 2023; "Apple slams UK surveillance-bill proposals", Zoe Kleinman, BBC, 20 July 2023.

at the IPCO. This is to ensure proportionality and necessity are considered before the review period has been set, and not after.

3. THE IPA SHOULD MAINTAIN THE REQUIREMENT FOR PRE-REQUISITE KNOWLEDGE IN THE USE OF INTERNET CONNECTION RECORDS FOR THE DETECTION OF HIGH-IMPACT OFFENDERS

3.1. The proposed amendments under the IPA to Internet Connection Records (ICRs) are too permissive and would remove certain safeguards that prevent unchecked government surveillance. The Act maintains certain pre-requisite knowledge, such as knowing the time of access by a user, or the service in use. However, the amendments seek to remove these, instead placing greater emphasis on necessity and proportionality tests.

3.2. Whilst we recognise the need for detection using ICRs, it is difficult to see how necessity and proportionality can be met with the potential widespread use of this new condition for the detection of high-impact offenders that would cover a longer period and a wider number of services.

3.3. This amendment would create digital dragnets without proper process to prevent the infringement of digital rights. Without knowing the time of access or the specific service accessed, such target detection would give rise to greater suspicion over a larger number of individuals which would be both counterintuitive to the purpose of the amendment and contribute to a presumption of guilt based on circumstantial evidence rather than evidence of wrongdoing.

3.4. The PBC should therefore maintain the requirement for some prerequisite knowledge to guide investigation of ICRs to prevent unnecessary and disproportionate infringement of digital rights.