Investigatory Powers (Amendment) Act 2024 Consultation Response to the Home Office

6 January 2025

Summary

We would like to commend the Home Office team on having done a great deal of work on the codes of practice and notices regulations. However, we believe that they still fail to address two significant and previously reported problems with the notices regime and the use of bulk personal datasets.

The act still includes powers that interfere with the ability of providers to offer strong encryption in their products, which in turn would harm the security of users not just in the UK, but around the world.

The act still sets too low a bar with regard to the use of bulk personal datasets: in our view, the concept of "low to no expectation of privacy" remains unsafe, especially in a rapidly-evolving technical environment characterized by machine learning and "large language models."

Analysis

Notices Regime

Two powers are of particular concern: the obligation for providers to notify the Secretary of State before making technical and other relevant changes to their products, and the requirement for providers to refrain from making any technical changes to their services pending the review of an appeal against a notice issued under the IPA.

First, while Annex I of the consultation draft excludes changes that "fix a defect in installed software and leave the intended functionality of the software unchanged," the fact remains that this power still requires providers to notify the Secretary of State of the addition of encryption to a previously unencrypted communications system, and makes it possible for the Secretary of State to veto such an addition. For example, had this power been in place in 2022, it could have been used to prevent Meta from improving the security of Facebook Messenger by adding end-to-end encryption to it.

Second, while Annex I also now sets an overall time limit for the Secretary of State to review a notice (180 days) and a further time limit to complete that review once reports have been received from the Judicial Commissioner and the Technical Advisory Board (30 days), we do not believe the Annex closes the remaining loophole to which we drew attention in our original consultation response. That is: if a provider appeals against the Secretary of State's decision on the issuing of a notice, there is still no time limit within which the Secretary of State must consider that appeal, let alone resolve it. This has the effect that, simply by doing nothing, the Secretary of State can force the provider to maintain the *status quo*, and, as suggested in the previous paragraph, prevent the addition of encryption to a previously unencrypted communications system.

As recent events in the United States have shown, the threat of hostile attacks on supposedly secure systems remains real: the "Salt Typhoon" security breach demonstrates that confidential communications are the target of well resourced, state-level attacks at mass scale. In that context, we believe it is counter to the UK's cybersecurity

interests to expect to veto either the addition of security measures to previously unencrypted systems, or the improvement of security measures in already encrypted systems. This is distinct from the category of "fixes to defects," since the intention of such additions would be to change (improve) the intended functionality of the system in question.

Bulk Personal Datasets

We do not believe that the measures set out in Annex A, on Bulk Personal Datasets, address the questions raised by then-MP Joanna Cherry KC, in her role as chair of the Joint Committee on Human Rights, on 6 March 2024.

In our view, the concept of a bulk personal [sic] dataset in which there is "low to no expectation of privacy" remains highly questionable, especially given "Factor (e)," as described in §4.20 of Annex A (p.13). Factor (e) "might be relied upon if the dataset has been widely used by industry…." We believe this is a dangerously low bar, at a time when so much personal data is being scraped by commercial third parties—usually without the individual's knowledge or consent—and used to train machine-learning or AI models. Such consentless use of personal data, regardless of how "wide" it is, should not be used to justify changing the privacy status of the data in question. *Nor do we believe that an individual has low to no expectation of privacy simply because their data is used to train machine learning models by the security services – contrary to the suggestion in §4.25.*

Recommendations

1 – Amend the notices regime so that the Secretary of State does not have a *de facto* right to veto the addition of security or confidentiality functionality to communications systems that do not already have it.

2 – Specify a time limit within which the Secretary of State must complete processing of a provider's appeal against a notice.

3 – Urgently revisit the concept of "low to no expectation of privacy" in the context of rapid evolution of AI/ML systems and the "scraping" of training data, and apply further safeguards via the Codes of Practice accordingly.

This response is submitted jointly by the Internet Society and the Internet Society UK (England Chapter)
January 2025