WRITTEN EVIDENCE FROM THE GLOBAL NETWORK INITIATIVE (GNI)

(IPA0009)

The Global Network Initiative (GNI), a multistakeholder organization focused on freedom of expression and privacy in the technology sector, expresses deep concern regarding the United Kingdom's (U.K.) proposed changes to the 2016 Investigatory Powers Act (IPA), as outlined in the Investigatory Powers (Amendment) Bill and requests that the Lords extend the period for and allow greater debate and deliberation on these changes.

GNI and its members have been engaged in UK surveillance policy for many years and have followed the IPA since it was introduced in 2016. We have previously provided substantive analysis on the U.K.'s primary policy governing the surveillance of electronic communications. While GNI recognizes the importance of protecting national security, we believe some of the government's proposed changes may significantly interfere with the privacy and safety of online users both within the U.K. and outside of its borders, and undermine the IPA as a model for emulation overseas. As this Bill enters the Report Stage in the House of Lords, GNI encourages the Lords to prioritize amendments that ensure an appropriate and proportionate scope of investigatory powers, inclusion of effective safeguards, sensitivity to jurisdictional reach and potential conflicts of law, as well as privacy and security safeguards.

Risks to privacy and security under Notification Regime

Proposed under Section 20, the new Notification Notice process empowers the UK Home Secretary - without the approval or oversight of a Judicial Commissioner - to legally require "operators that provide lawful access of significant operational value" to proactively inform the Home Office of their intentions to make certain adjustments to certain products or systems. Details as to the types of services and changes requiring notification remain vague. Notices will be issued in secret, without the ability for operators to alert anyone to their contents or existence, and proprietary to each operator. Section 17 further mandates that operators refrain from making certain alterations to their services or systems if they have been served with data retention, national security, or technical capability notice. This restriction applies even if the notice is under review and has not yet been fully implemented.

These requirements represent a burdensome and unprecedented assertion of state control over the information and communications technology industry that will impact companies' ability to operate and innovate freely in a global market. Many of the technologies covered by these requirements are deployed to avoid or mitigate cybersecurity risks, comply with relevant data protection laws and regulations, and ensure smooth and consistent user experiences. The act of having to notify and explain proposed technical changes *prior* to their implementation potentially increases risks to cybersecurity, enhances the potential for conflicts of laws, and is likely to lead to the degradation of user experiences. Paired with existing powers to give other types of Notice,

this could allow the UK government to pre-emptively and indefinitely delay the rollout of new products and services in the UK market. This is a significant change to the current regime with significant consequences, likely to be further amplified as other governments, including authoritarian regimes, seek to mirror the same authority in their domestic legal frameworks, citing U.K. precedent.

Furthermore, the notice regime raises serious concerns regarding the potential for government overreach and infringement of privacy rights. By mandating pre-notification (Notification Notices) for planned changes to services or products, these amendments grant the U.K. Home Office extraordinary awareness and control over tech providers' operations. Such sweeping powers, unparalleled in their scope, pose a significant threat to future product security and consumer privacy globally. Additionally, the Bill raises the specter that the U.K. government could force companies to continue offering products with known security or privacy flaws, hindering their ability to improve products over time in response to evolving regulation, external threats, and market expectations or decommission obsolete, flawed or unsecure products and services.

We do not see this as a debate about "encryption" per se - but rather the wider issue of companies' ability to innovate to advance the data protection, data security, and data minimization efforts expected by users and governments globally.

We encourage the UK government and the Lords to carefully consider the implications and practicality of these provisions and opt instead for other less restrictive, burdensome, and costly approaches to achieving relevant, legitimate national security objectives. If a notice regime is to be imposed, the Bill should be amended to significantly narrow its application, impose sufficient transparency and accountability mechanisms (see below), and create exceptions for critical privacy and security-related adjustments.

Extraterritorial impact

The UK government asserts that other provisions of the IPA already have extraterritorial application. For instance, under Section 253(8), a technical capability notice "may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom)."

The Bill seeks to broaden the extraterritorial reach of the legislation not only via the new Notification Notice but also by revising the definition of "telecommunications operator" to encompass a wider range of individuals or companies engaged in providing telecommunications services in the U.K., including those that manage or offer telecommunications systems situated outside the U.K.'s borders. This would effectively mean that a Technical Capability Notice or National Security Notice issued by the U.K. could impact global product improvements.

Alternatively, a provider facing such a notice might be incentivized not to introduce an update or to withdraw its product or service altogether from the U.K. market.

The Home Office has acknowledged that the Bill may raise conflicts of law between the U.K. and other countries, including the U.S. and EU. Unlike the IPA itself, there are no mitigations[1] and overseas providers are exposed to an unquantified risk of extraterritorial enforcement by a foreign government. The Notice regime imposes a strict non-disclosure obligation on companies, preventing them from informing anyone, including the public or the US or EU member state governments, about a Notification Notice or Technical Capability Notice. Specifically, companies are prohibited from disclosing the existence or contents of the notice to any third party without the express authorization of the U.K. Secretary of State. This blanket gag provision effectively shields these orders from scrutiny and impedes the ability of other governments to be aware of, review, or intervene in these decisions. It also prevents overseas companies from seeking diplomatic assistance from their domestic government in the event of an overreach of power or a situation where a UK notice puts an overseas provider in breach of legal obligations or orders stemming from another jurisdiction.

By asserting extraterritorial jurisdiction and providing no mitigations against enforcement, the Bill could also provide unintended justification for similar actions by other governments, especially authoritarian regimes already pursuing legislation that would hinder companies' ability to transfer data across borders and protect users from government overreach. The combined effect of broader and more explicit assertions of extraterritorial jurisdiction, paired with threats of enforcement, increase the likelihood of conflicts of laws and further complicate the international legal framework applicable to technology providers at a time when the stated and shared objective of the UK government and other key stakeholders is to protect the open, interoperable, secure, and global internet from threats such as unwarranted surveillance and unnecessary fragmentation.

We urge the Lords to consider carefully the broader ramifications of introducing such broadly framed and unilateral extraterritorial powers and enforcement, and to scale back their application, including by forbearing from notices which create conflict of law scenarios.

Transparency and accountability

As a member of the Freedom Online Coalition, the U.K. has committed to promoting "transparency and independent, effective domestic oversight related to electronic surveillance." The Bill in its current form misses the opportunity to fulfill the state's commitment to greater transparency and accountability regarding its surveillance practices. As stated in the FOC

[1] Under the IPA, the UK government forebears from extraterritorial enforcement where overseas companies operate under an international agreement, such bilateral agreements with the US government under the CLOUD Act.

guiding principles on government surveillance, governments should ensure the operation of surveillance technologies is governed in a manner that proactively mitigates the risks of misuse and enables appropriate access to judicial or administrative review. The Bill lacks substantive safeguards against government overreach by allowing for the more permissive use of bulk data by U.K. agencies where there is "low or no reasonable expectation of privacy" without judicial authorization. Introducing this vaguely defined category of "bulk personal dataset (BDP)" allows agencies to justify accessing and processing data without proper safeguards, even when individuals have a reasonable expectation of privacy in their personal information.

GNI recommends that governments disclose information about the bulk data demands they make on operators, including the number of warrants, the number of users affected by those demands, the specific legal authority for each of those demands, and what type of content the agencies sought under BDP requests. Companies should also be permitted to disclose the number of notices that they receive, how they respond to them, and the technical changes they are legally bound to install, implement, and comply with. We urge the U.K. government to consider how users can have meaningful redress without transparency about authorized intrusions into their privacy.

Conclusion

For reasons outlined above and echoed by industry stakeholders, the amendments are disproportionate, potentially harmful to users, and unworkable, and as such likely to lead to significant impacts on privacy and security in combination with existing powers. We remain very concerned about the proposed changes to the notice regime, the lack of safeguards and mitigations, and the global implications of such measures.

To ensure that the U.K. acts consistently with its international obligations and that it protects privacy and communications security, we ask that the Lords ensure that any amendments to the IPA (1) do not hamper or delay the rollout of new privacy and security measures, (2) do not create or exacerbate conflicts of laws problems, (3) promote transparency about surveillance demands, (4) retain judicial control over bulk data demands, and (5) extend the period for deliberation of the legislation to permit consideration of such changes to the proposed amendments to the IPA.

(7 February 2024)