Rt Hon Suella Braverman KC MP
Secretary of State for the Home Department
Home Office
Investigatory Powers Unit
2 Marsham Street
London
SW1P 4DF

Via email to IPAnoticesconsultation@homeoffice.gov.uk

31 July 2023

Re: Consultation on revised notices regimes in the Investigatory Powers Act 2016

Dear Home Secretary:

On behalf of the Software & Information Industry Association (SIIA), the principal trade association for those in the business of information, we write to provide feedback regarding the proposed revisions to the notices regimes in the Investigatory Powers Act 2016 (IPA). SIIA represents over 450 companies in academic publishing, education technology, financial information, software, platforms used by millions worldwide, and data analytics and information services. We represent organizations based in the United Kingdom (UK) along with many organizations that do business within the UK. Our mission is to protect the three prongs of a healthy information environment essential to that business: creation, dissemination, and productive use.

SIIA supports the law enforcement community's desire to possess every practical and ethical tool at its disposal to pursue bad actors. Unfortunately, the revised notices regimes outlined in this consultation will do far more harm than good to the very consumers the IPA's already sweeping investigatory powers are meant to protect. In this case, we believe the direct impact on consumer's rights and freedoms, as well as the harmful effect such changes are likely to have on technological development in the UK, would catastrophically weaken UK citizens' safety and security.

The consultation sets out several goals upfront: to strengthen the notice review process, expand the scope of the regime, and introduce new notice requirements. Yet the consultation's ministerial foreword frames the proposed revisions as "not about the creation of new powers, [but] about the efficacy of long-standing powers the necessity of which has long been established."[1] Unfortunately, this premise is precisely the problem. The revised notices regimes, for example, suggest combining government pre-clearance of new technologies and additional control over extraterritorial entities. Among other challenges, this would force domestic and even foreign companies to decide between enabling the UK to veto security services provided worldwide–since, effectively, allowing one authority with means to step through a security gate creates a vulnerability that can be exploited by

[1] UK Home Office, "Investigatory Powers Act 2016 Consultation: Revised Notices Regimes" (5 June 2023) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1159672/Revised_notices_regimes_consultation.pdf).

malicious actors–and ceasing operations in the country. It would also render the Home Office the de facto regulator of technological development for companies that sit outside the UK. The 2018 IPA Technical Capability Regulations do not limit notices presented to non-UK companies to only UK persons. Therefore, as long as even a relatively minor subsection of a service provider's users is located in the UK, a notice under the revised regimes could force compliance and weakening of privacy standards worldwide.

Compounding this marriage of inconveniences is the proposal to force compliance with a notice even before completing the review process mandated by the IPA. This effectively guarantees that consumers across the world would be left exposed in cases where these now-unreviewed requirements unintentionally open cybersecurity vulnerabilities – at a time when cybersecurity threats are only increasing.

I. **Requiring pre-clearance of changes to product security features before they are released threatens UK and global consumer privacy and security and would dissuade a host of societally beneficial technological developments.**

Enabling the Secretary of State to require service providers to clear technological innovations with the Home Office would, first and foremost, chill the development of new technologies. The majority of the harm to development would apply to technologies, such as end-to-end encryption, designed to *enhance* consumer privacy and safety across the world. Indeed, the proposed revisions would give the UK a power no other Western government possesses: prohibition on technological development in the name of government access to private data. In addition to the clear anti-privacy implications of such a regime, the uncertainty surrounding approval of privacy-enhancing technologies (PETs) would naturally dissuade investment in their development, contrary to the UK's objective of promoting PET adoption, as reflected in extensive work by the Information Commissioner's Office.[2]

If any company is unsure whether a technology will even see the light of day, it is unlikely invest in creating or bringing the technology to the UK, even if the technology is critical to protecting consumers against modern cybersecurity and privacy threats. The upshot is to limit the technologies available to British residents. Even if the Home Office intends to use a "light touch," companies will not have enough clarity on how the law will be applied and will be reluctant to take a chance and hope for the best. Moreover, the pre-clearance requirement will do nothing to prevent cybercriminals from continuing to develop new and innovative ways to breach existing, yet increasingly stale, security measures.

The proposed pre-clearance requirement would also have negative implications for speech within and outside the UK. If the Home Office declines to approve technology that maintains or plugs gaps in existing cybersecurity networks, especially end-to-end encryption, it would undermine the privacy of UK citizens' data as well as potentially expose the data of foreigners who rely on these privacy

[2] *See, e.g.,* Information Commissioner's Office, "ICO urges organisations to harness the power of data safely by using privacy enhancing technologies" (19 June 2023) (https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/06/ico-urges-organisations-to-harness-the-power-of-data-safely-by-using-privacy-enhancing-technologies/).

measures for their personal safety. These include citizens subject to authoritarian regimes, including political dissidents, journalists, and human rights advocates.

In fact, it is easy to see how such a change to the UK's IPA could encourage authoritarian governments—and even democratic governments—to grant themselves similar powers over technologies operating in those jurisdictions. While authoritarian governments are unlikely to prioritize the development of PETs, they will jump at the opportunity to reduce consumer privacy measures that hamstring the ability to obtain user data for anti-democratic purposes and social control. Even if the UK uses a light touch in vetoing potential technologies, these foreign actors will not.

II. Requiring non-UK-based companies to comply with changes that would affect their product globally, such as providing a backdoor to end-to-end encryption, would spell disaster for consumer privacy and force companies to avoid offering encrypted products and services to UK consumers.

We are particularly concerned that the revised notices regimes would weaken end-to-end encryption and create a backdoor. Though the driving force for this change–improving the data available to law enforcement and intelligence–is laudable, the effect of weakening encryption protection will create privacy and cybersecurity problems that we believe will have significant repercussions for individuals, the UK economy, and international security. Encryption protects not just government and commercial databases, but critical national infrastructure such as hospitals, airlines, and nuclear power stations – exactly the targets terrorists would attempt to hack and destroy. Furthermore, if the UK government gained backdoor access to encrypted material, it is almost certain that other governments and non-government actors could exploit that vulnerability, rendering encryption useless. In other words, it is impossible to create a backdoor that only the "good guys" can use.

Even if companies were willing to weaken international cybersecurity and PETs to comply with such a notice, the proposed regimes would trap them between the Scylla of the IPA and the Charybdis of Europe's General Data Protection Regulation (GDPR) and the CLOUD Act in the United States. For example, privacy-invasive notices would infringe on Article 32 and Recital 82 of the GDPR, which respectively require measures to protect user privacy and permit encryption as an acceptable means. For its part, the CLOUD Act bars mandating the decryption of consumer data as a component of data sharing agreements, yet a notice demanding this would force companies operating in the UK and the United States to do just this.[3]

As a result, multinational companies—even those operating outside the UK—would be forced to balance the value of end-to-end encryption to their consumers *and* conflicting mandates in other jurisdictions with the revised notices regimes. The result is that most will likely be forced to cease doing business in the UK market, unnecessarily leaving UK citizens without the evolving cybersecurity and privacy protections enjoyed by citizens of other countries.

[3] *See* 18 U.S.C. § 2523(b)(3).

III. Requiring immediate compliance with a notice would lead to technically infeasible notice requirements by removing critical guardrails and, along with the pre-clearance and extraterritoriality proposals, create unprecedented and unworkable outcomes.

The final proposed change would mandate compliance with notices even before the Secretary of State, Judicial Commissioner, and Technical Advisory Board complete their review processes. These checks were implemented into the IPA as a necessary check on the notice power and the otherwise significant consequences that could stem from receiving one. Even on its face, requiring compliance in advance of findings that notices are technically workable and proportional would effectively render this process protection toothless: the costs, feasibility and effects on consumers would already be felt by the time a decision is rendered. In the context of the pre-clearance and extraterritoriality proposals, the removal of this protection is even worse.

Taken together, these proposed changes would permit the Home Office to unilaterally issue a notice to a foreign company to reduce the protections provided to global consumers via end-to-end encryption. This unprecedented power is made even more unworkable given the existing requirement in the IPA that a notice's recipient maintain confidentiality and avoid disclosing the notice. This means companies could be required to diminish UK and worldwide users' privacy and retain the capacity to produce unencrypted data or simply delay security updates – all in secret due to the IPA's gag order regarding the requirements of the notice. In addition to the damage such unbeknownst requirements would do to consumer privacy, some software updates cannot legally be made without public disclosures, again placing service providers in an impossible position. Without delaying implementation of notice requirements until review is complete, however, there is no way of assessing this feasibility (this is, in part, the purpose of the review process in the first place).

* * *

Thank you for considering our views. SIIA consents to publication of our comments with attribution. Please contact us with questions on this feedback.

Respectfully submitted,

Paul N. Lekas
Senior Vice President, Global Public Policy & Government Affairs

Anton J. van Seventer
Counsel, Privacy and Data Policy