**Revised Investigatory Powers Act notices regime**

techUK response

July 2023

About techUK

techUK is a membership organisation launched in 2013 to champion the technology sector and prepare and empower the UK for what comes next, delivering a better future for people, society, the economy and the planet.

It is the UK’s leading technology membership organisation, with more than 950 members spread across the UK. We are a network that enables our members to learn from each other and grow in a way which contributes to the country both socially and economically.

By working collaboratively with government and others, we provide expert guidance and insight for our members and stakeholders about how to prepare for the future, anticipate change and realise the positive potential of technology in a fast-moving world.

**Introduction**

The UK government has made it a strategic priority to promote the country as a supportive nation for innovation and technology, as evidenced by the £370 million in new funding that has been committed by the Prime Minister’s Science and Technology Framework and the Government’s aim to make the UK a Science and Technology Superpower.

To maintain the UK’s competitiveness as a world-leading hub for innovation it is crucial to consider any changes to the Investigatory Powers Act (IPA) 2016 carefully. Failing to do so could risk contradicting the essence of the Prime Minister’s plan for innovation, and could raise doubts among companies about the UK’s suitability as an investment destination or market for their services. Additionally taking the right approach on reform will be vital to maintaining the UK's international reputation as having high-quality regulation that can meet both public policy outcomes while supporting a positive business environment. Currently techUK members are concerned that the reforms proposed to the IPA in this consultation run the risk of both damaging the UK’s suitability as a market to operate in as well as harming the perception of the UK as a jurisdiction that takes a balanced and proportionate approach to regulation.

The IPA sets out statutory powers used by public authorities, including law enforcement and the UK intelligence community, to obtain communications data. This includes the notices regime which provides for three different kinds of notices that can be imposed on service providers falling within the IPA's scope: data retention notices, technical capability notices and national security notices.

techUK and our members welcome the government’s decision to consult early on potential reforms to the IPA. We appreciate the UK government’s established tradition of industry consultation, independent expert review, and thorough parliamentary consideration prior to making significant changes to the IPA regime. Indeed, the Home Office’s review of the IPA in February noted the extensive industry and expert input, as well as parliamentary considerations, as principal basis for the IPA’s success and legitimacy. The UK government recently built on this tradition, commissioning Lord David Anderson to conduct an independent review of the IPA, which was completed last month.

We share views expressed by Lord Anderson in his review, emphasising that any proposed changes to the Act should undergo thorough debate, analysis, and parliamentary scrutiny. This consultation document has thrown up a range of unanswered questions as well as further issues that need to be explored. techUK and our members are committed to working with the Government as the consultation progresses and would welcome and be able to support further engagement between the Home Office and tech UK tech sector.

Indeed, techUK and many member companies have a history of engaging with the government and Parliament during the passage of the IPA. This consultation revisits several core issues that were robustly debated at that time, including proportionality and transparency, territorial scope, and enforcement.

It is imperative to ensure that the operation of the legal framework governing the IPA regime safeguards the legitimate aims of national security and public safety without compromising the privacy or security of the internet, or its users (including end user enterprise customers and consumers). It is also critical, as our members have indicated in previous submissions on investigatory powers, to recognise that user trust is essential to our members’ ability to continue innovating and offering products and services that empower individuals in their personal and professional lives, including through offering improved privacy, security and safety measures like end-to-end encryption.

Any legislation that is passed by the UK may also serve as a model for other countries, including with respect to UK citizens’ data. Therefore, it is imperative that a notices regime is underpinned with robust end-to-end safeguards, and overseen by an independent oversight authority. The proposed regime for amended notices regime should not weaken the previously established legal and other safeguards placed in the UK to ensure data privacy of customers and consumers.

Ensuring this will support the UK’s ambition to remain the best place in the world to start and grow a tech business. In the Ministerial Forward, it is stated, “this consultation is therefore not about the creation of new powers, it is about the efficacy of long-standing powers the necessity of which has long been established”. However, we believe that this understates the significance of what is being considered here.

Some of the objectives set out in the consultation have the potential to be very far-reaching, and negatively affecting techUK members’ ability to innovate their services for their users globally, including to improve the privacy, integrity and security of their services. Additionally, it would exacerbate conflicts of laws that governments should aim to resolve, and undermine user trust.

Given the high-profile review of the UK’s surveillance regime in 2014-2016, which involved avowing powers and modernising the authorisation process and safeguards for individuals, it is crucial that this and future reviews maintain the same degree of transparency and openness. Any changes made by the UK will be closely watched by other governments; thus, it is vital that they meet the same high standard and are worthy of emulation overseas.

The consultation notes that some of the objectives could be achieved through different routes, but these other routes are not set out in the document. We would encourage the government to provide specific examples of and consult on these alternative routes so that members can evaluate them alongside those included in the consultation.

techUK appreciates the Home Office’s engagement with us ahead of responding to this consultation. We value the collaborative approach taken thus far. However, the specific problems these proposed changes aim to address remain unclear, making it challenging to gauge their necessity and proportionality. This lack of clarity gives rise to numerous questions, including the underlying factors that have necessitated a review of the existing powers.

Additionally, there is uncertainty regarding whether the new changes could enable the government to issue notices to types of providers that have not previously been subject to one, such as the digital service providers. Therefore, we would greatly appreciate further engagement to clarify these points to better understand the implications of the proposed changes and their potential impact on techUK’s members’ operations and services. Resolving these uncertainties is crucial to ensure a comprehensive and well-informed response.

Finally, we would be grateful if the government could provide a more detailed timeline for the consultation process and confirm that members will have further opportunities to provide their input.

techUK has provided a number of reflections on the objectives highlighted in the consultation:

## Objective 1 – Strengthening the notice review process

Government proposes that the terms of a notice - when given for the first time - should apply while the Secretary of State is reviewing the notice following a request by the service provider.

When the IPA was implemented, its powers were keenly debated in Parliament and the UK government cited robust procedural safeguards, including the referral process (s. 257) as a balance on its powers, including the notices regime.

The s.257 referral back period is critical, allowing service providers to dispute a notice, requiring the Secretary of State to consult with the Judicial Commissioner and Technical Advisory Board on the notice's lawfulness while knowing that, pending the outcome of that process the notice remains suspended in its effect.

Removing this procedural safeguard, in particular proposing that operators should be prohibited from making changes to their products or systems while their review request is being considered by the Secretary of State, does not follow regular due process and could weaken consumer privacy and security protections where important updates are needed.

Operators may want to appeal a notice for various reasons, such as its due to concerns over its lawfulness, workability, breadth, concern over the impact on a company’s users or due to it being unduly burdensome.

The absence of an appeals process makes it challenging for companies to challenge the appropriateness of the request, leaving them with no recourse if they find the notice to be inappropriate or burdensome. The existing appeals process ensures a balanced approach and mitigates these concerns before the operator is bound to comply. Additionally, the proposed changes, could place companies in a challenging situation where they are required to disable or block a new product feature, notwithstanding the fact the notice is under review. In some cases, this could lead to disparities between features available to UK users and those available elsewhere in the world, potentially causing irreversible harm.

Companies frequently introduce numerous features and products across multiple global regions to cater to the needs of thousands of customers annually. We believe that imposing a requirement of this magnitude could pose significant challenges. It is essential to strike a balanced approach that considers the potential impact on businesses, regions, and customers relative to the specific notice in question. Given this is a significant departure from the original approach taken in the IPA regime we believe the Government needs to explain further the reasons for such a change and to justify to Parliament why the withdrawal of this safeguard is necessary.

## Alternative, more proportionate approaches could be considered such as an obligation to preserve data in question.

## Additionally, we would welcome clarification on the maximum review period.

## Objective 2 – Timely and informative responses

Government proposes under this objective to oblige providers to engage in the consultation process before a decision to give a notice is made or with any subsequent review process, and to provide relevant information to the government as necessary and within a reasonable time.

Constructive engagement with the government, in a timely manner, on matters of national security is in the interests of most companies, as it ensures that the relevant decision makers can make fully informed decisions. However, many of our members are uncertain about the terms and duration of such cooperation, as well as the authority responsible for assessing compliance. It is also unclear whether the intention behind this proposed is to encourage the sharing of specific confidential information or to set forth specific time requirements for cooperation and information sharing. Members would also like to ask for additional clarification around what kind of *“technical information”* the companies would be compelled to share, and whether this obligation would also mean there would be non-compliance linked penalties. techUK and our members would like to stress that this requirement should be proportionate.

To help us better understand the aims of this proposal techUK would welcome clarification on whether any particular challenges have been identified in the existing system that necessitate turning this into a legal obligation on operators.

## Objective 3 – Scope of the regime

The consultation contemplates *“changes to the Act to provide greater clarity that its provisions continue to apply to the operators to whom it was intended to apply, including those that have adopted more complex corporate structures”* and to *"strengthen enforcement options"* accordingly.

techUK and our members hold significant concerns regarding the government's proposed expansion of the notices regime scope. This objective proposes to reassert UK jurisdiction over providers operating overseas under another jurisdiction, with the addition of strengthened “enforcement options”.

Given this significant step we would like to understand the extent to which this has been discussed with the governments likely to be impacted, in particular the US and Ireland, and what enforcement options are being considered.

The definition of telecommunications operator was carefully enacted by Parliament, who considered the global nature of technology companies and the extra-territorial application of the IPA. The chosen approach was to ground it by applying to operators, including overseas operators, offering or providing *"a telecommunications service to persons in the United Kingdom"* or operating a telecommunications network in the UK.

This objective proposes to reassert UK jurisdiction over providers operating overseas under another jurisdiction. Moreover, it appears to suggest that a notice could be served on more than one entity, including entities other than the one providing the service to users (for example, the service provider and the upstream cloud provider).

This would undermine the principle established during the Bill stages, where agencies should engage the entity that is closest to the user and would interfere with the public commitments many international providers have made to be transparent about how they respond to government requests for access to user data.

In the area of national security and law enforcement, it is inappropriate to depart from a jurisdictional nexus limited to the UK; to do so infringes upon the sovereignty of other nations, their rule of law, and users’ expectations in those countries not to be surveilled by foreign governments. Our members have long advocated that the only right solution here is diplomatic agreement with governments of other countries concerned. The proposed clarity does nothing to resolve conflicts of law; instead, it exacerbates the issue and could make the UK a less attractive place to provide technology services.

Additionally, we would welcome further definition of the term “*complex corporate structures,*” the specific concerns the government has regarding them, and, once the government has fully considered the existing precedent in wider UK legislation, an elaboration of the phrase "*strengthening enforcement options.*"

Given that these are extremely complex and novel legal matters regarding the balance between fundamental rights and national security, we believe that fines would be an inappropriate response. Fines are typically used in regulatory matters, and we believe that a more nuanced approach is needed in this case.

We would like to understand how the the proposed power be used and whether a notice could ever require a company not to launch a particular feature or product to UK users or to legally restructure their business, and whether such requests could be made retrospectively - i.e.: could a notice require a company to modify or withdraw something that is already in the market.

## Objective 4 – notification requirements

This objective seeks to introduce a stand-alone obligation on “relevant operators” to “where necessary”, notify planned “relevant changes” to the Secretary of State, even where no prior notice has been given. techUK appreciates acknowledgement that the impact on commercial decisions should be taken into account, which is a particular concern for our members with international operations. However, we have serious reservations about this proposal and its potential impact on national security, user rights and safety, and operators’ freedom to conduct business and innovate their services.

We note that the notification process already exists in the regime, but it is not clear that these notices have previously been served on the types of companies that this consultation seems to intend to. Therefore, we would welcome more information on this point. We would also note that the proposal targets this power only at operators and changes that are “relevant”. We would ask for more detail as to what would be considered “relevant” and further clarity on the “thresholds” being considered.

Additionally, the proposal suggests that the required notification should be made within a "*reasonable amount of time*." We understand that the government intends to rely on a definition, set out in the *Investigatory Powers (Technical Capability) Regulations 2018 ((Schedule 1 paragraph 13, Schedule 2 paragraph 13 and Schedule 3 paragraph 11)*. However, the definition provided in these provisions is silent on what specifically constitutes a “reasonable amount of time,” leaving scope for interpretation. We would ask the government to provide a specific timeframe deemed as "*reasonable.*"

The requirement also appears to encompass common product and service developments that improve privacy and security for consumers, businesses, and the government. This would likely create vulnerabilities in data security protections for customers and consumers. For example, providers serving government entities in the UK require the highest standard of security to protect against unlawful access to government data. Providers must have the flexibility to make immediate changes to services to protect user data from intrusion or cyber hacking threats by bad actors. Delaying changes in order to undergo a notification process to the Secretary of State would give bad actors more time to exploit vulnerabilities. It is also unclear whether the proposal would apply to changes that operators make to their systems to meet compliance obligations or contractual obligations to customers.

Furthermore, requesting companies to share information about their planned changes is highly impractical. Companies normally deal with an array of ongoing potential changes to their systems, making it cumbersome to not only track and identify each planned change but also evaluate to ascertain how each could impact the government’s ability to exercise its investigatory powers. The expectations associated with such a requirement are also unreasonable and unworkable in that operators do not necessarily know what changes to a service could affect the efficacy of investigatory powers notices. Additionally, this requirement raises concerns about the potential disclosure of confidential information and the potential impact on feature and product development rollout if there is a lack of alignment with the government's preferences.

It would be helpful to gain more clarity on the government's intentions regarding the handling of such notices and information. Specifically, we are interested to know if the government intends to engage with operators to negotiate how they develop and roll out their services and systems.

Moreover, the timing of such notification is unclear, as it raises the questions of what stage the companies would be expected to notify the Secretary of State. For example, would such notification be expected to occur at the point when the product is ready to be rolled-out, or at such an early stage where not all details regarding the implementation of a new feature have been considered. In the case of the former, we would like to note that, by the time a product can be considered ready to be introduced, significant time and resources would have gone into its development and testing, making such an approach financially burdensome.

During the passage of the IPA Bill the government explicitly recognised that operators, where no existing notice had been issued, were not required to notify the government of any planned changes to their systems. This decision was emphasised as a measure to avoid placing undue burdens on businesses. Given this context, we seek clarity from the government on the reasons behind deeming such a provision necessary at this point. Understanding the rationale behind this change will help us better grasp the government's current position and the factors that have influenced this shift in approach.

Overall, an “expectation” to notify the UK government of product changes could create an unwieldy and expensive notification regime, imposing disproportionate duties on the operator and stifling innovation and unduly constraining the ability of operators to implement capabilities intended to protect their customers from cyber hacking threats which compromise their privacy and data security. Any associated enforcement could also push businesses to over-report and therefore present a logistical burden for the government to manage as well.

Apart from the practical difficulties of policing such a regime and the need to avoid UK government overreach, it is equally important to consider the potential impact on the UK’s global standing as an innovator in the tech industry. This requirement could potentially differentiate the UK from other nations negatively, as a country that is not supportive of or invested in innovation. For example, certain providers may opt to discontinue offering their services in the UK, while others may provide only limited offerings, or less secure services that allow UK customers to communicate only with other UK customers. This scenario could result in UK consumers having limited access to the global market and losing access to many of the world's most secure products and services. Hence, it is crucial to carefully evaluate the implications of such a measure.

In light of these complexities, members encourage the Home Office to continue engaging in a dialogue with the industry and to clearly set out specific and focused areas of concern. This would allow the government adopt a more targeted approach that is focused on particular areas of sensitivity and will present a more feasible and effective solution.

Given the potentially very wide scope of these powers, combined with the proposals to expand the scope of this regime, we would urge the government to set out clearly the case to Parliament for why such powers are necessary and proportionate, and what safeguards are being considered.

Further to this the Home Office needs to provide significantly more clarity on how any such envisaged powers would operate in practice.

## Objective 5 – Renewal of notices

This objective seeks to introduce a statutory role for the Investigatory Powers Commissioner in decisions to renew notices once they are in place. techUK sees a rationale for undertaking this change. However, we would appreciate further insight into how this process would work as compared to what is currently in place, the objectives behind introducing a statutory role for the Investigatory Powers Commissioner, and why only with renewals and not new notices.

## Other comments

While our members are familiar with data retention and technical capability notices, national security notices were not discussed with key groups of members during the Bill stages, particularly with digital service providers. We would therefore welcome the opportunity for these stakeholders to engage with the government on this important topic during the current consultation process. We would be happy to facilitate this discussion.