WRITTEN EVIDENCE FROM FREEDOM FROM TECHUK (IPA0010)

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 1,000 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 Investigatory Powers Act (IPA) 2016 sets out statutory powers used by public authorities, including law enforcement and the UK intelligence community, to obtain, retain, and examine communications data. The IPA 2016 was legislated for after a lengthy period of debate about how to safeguard national security while also respecting individuals' fundamental rights and embedding safeguards including transparency and judicial authorisation. The end result was a regime that allowed authorised agencies to seek lawful access to data and to give notices where necessary and proportionate. IPA also contains world-leading safeguards which have made it worthy of emulation overseas.

The government now proposes amendments to the IPA 2016 through the Investigatory Powers (Amendment) Bill 2023. Achieving a balanced and proportionate approach to reform will be vital to ensuring 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, security, or safety of consumers. Additionally taking the right approach on reform will be vital to maintaining the UK's international reputation as a jurisdiction that takes a balanced and proportionate approach to regulation that is supported by strong accountability mechanisms.

The government has stated that the changes set out in the IP(A) Bill seek to protect the existing capabilities that keep our citizens safe. techUK and our members support the legitimate aims of enabling investigatory powers that are necessary and proportionate to keep citizens safe.

However, we are of the view that the proposed reforms raise concerns about government intrusion of user privacy – a fundamental human right – by hindering technological advancements aimed at improving consumer privacy, integrity and security through technologies like end-to-end encryption. Moreover, these changes are also problematic due to

their potential to exacerbate and/or create conflicts of laws, without clear mitigation plans. If emulated by other nations, these changes could have global repercussions, with potential impacts on human rights both in the UK and internationally.

In this submission, techUK outlines our members' concerns around the proposed changes to the notices regime, detailed in Part 4 of the IP(A) Bill.

1. **Implications on data privacy and safety in the UK and internationally**

Currently, to issue a notice under the IPA 2016, the Home Office is obligated to consult with the operator. The consultation is not bound by defined parameters or length, but it typically involves discussions with the company during the drafting of the notice. If the decision is to proceed, the notice goes through a double lock process, requiring approval by the Home Secretary and a Judicial Commissioner before it can be given to the operator in question. Once the notice is given to the company, it has a 28-day window to request a review by the Secretary of State. The IP(A) Bill makes the following changes to the original Act:

- **Clause 18 (*Review of notices by the Secretary of State*)** sets out that during the notice review period, operators are prohibited from making changes to their systems and products if they negatively impact Home Office's existing lawful access. It also introduces a requirement for the Secretary of State to set out and comply with a time limit for reviewing the notice.
- **Clause 21 (*Notification of proposed changes to telecommunications services etc*)** will introduce a new type of notice – the Notification Notice which, upon issuance, would require specified operators to notify the Home Office of plans to make product or system changes to a yet-to-be-defined list of services that will be private and unique to each company.

techUK members are concerned that, when used in combination, changes introduced by these two clauses would grant the UK government a de facto power to veto companies from making changes to their global products and services offered in the UK and internationally.

This could impede the ability of techUK members to modify products and services over time to protect users from active security threats, to innovate, and enhance their services for their users. This may result in unaddressed vulnerabilities in data security protections for consumers. Instead of focusing on improving user privacy and security, firms' attention would have to be diverted towards fulfilling the surveillance needs of the UK government.

In turn, this could differentiate the UK from other nations negatively, as a country that is not supportive of innovation, creating a disincentive for companies to provide their services in the UK, potentially restricting what features are made available in the future.

For example, certain providers may opt to discontinue offering their services into the UK, while others may provide only limited offerings, or less secure services. This scenario could result in UK consumers losing access to many of the world's most secure products and

services. This is of particular concern in the world where threats to users' data security continue to grow.

As a hypothetical example, if these new powers are used to restrict operators' ability to innovate safety measures like end-to-end encryption, it could have profound societal repercussions for users both in the UK and globally.

Encryption plays a crucial role in providing a secure exchange for oftentimes sensitive and confidential data across various public and private domains. For instance, doctors, lawyers, and accountants utilise it to transfer sensitive information securely, ensuring both adequate protection and compliance with data protection legislation, such as the General Data Protection Regulation (GDPR). Encryption also provides a defence mechanism against unwanted intrusions, and criminal activities, safeguarding data from potentially disastrous breaches, particularly when the compromised data is of a personal nature.

Consumers value private channels to communicate and will actively choose more secure services with an eye on protecting their rights. techUK members have stressed to us the importance of being able to provide secure services for consumers across a range of markets and that in key markets ensuring privacy is a central selling point.

End to end encrypted services also often serve as an indispensable tool for journalists and activists across the world, protecting them from bad actors by enabling them to engage in confidential communication, in turn ensuring their physical safety and protecting their right to freedom of expression. Repeatedly these services have been used in scenarios where human rights have come under threat, such as for whistleblowers and refugees and in response to major events such as after the breakout of war in Ukraine.

Maintaining access to service such as these are therefore hugely important both for consumer choice and broader issues of safety. It is therefore essential to bear in mind that these reforms, despite being portrayed as a solely domestic initiative, have the potential to bear adverse outcomes globally, posing a risk to online security on a broader scale. Thus, robust end-to-end safeguards and accountability mechanisms are crucial to ensure responsible implementation.

Ensuring strong accountability measures within the Notifications Notices regime

As set out above, the government has made changes to the IP(A) Bill to introduce a requirement for the Secretary of State to establish, and comply with, a time limit for the review of notices, and committed to a public consultation on regulations that will set out these timelines.

Government has introduced welcome amendments to limit the length of the notice review period. However, given the scale of the changes being proposed, and their potential impacts on the human rights, more needs to be done to ensure the updated regime is transparent, proportionate, and contains a robust accountability mechanism.

This clarity is needed on the face of the Bill, as well as further clarity from the government on what information the Secretary of State will be required to take into account when setting the timelines for reviewing the notice, and whether there will be an appeals process for operators to appeal the decision in regards to the length of the review, in case they deem the review period to be too lengthy.

Furthermore, additional safeguards should be built into the regime, including a clear definition of "relevant changes" that would have to be notified – either on the face of the Bill, or in the secondary legislation.

Concerningly, and unlike the existing three types of notices, a notifications notice would be approved by the Home Secretary alone and not need to go through a 'double lock' process, which requires the approval by the Home Secretary and a Judicial Commissioner before it can be given to the operator in question. Therefore, it will be important to ensure that the notifications notices are subject to the 'double lock' authorisation process, in line with the procedure for approving the three existing notices in the IPA 2016.

2. **Exacerbation of conflicts of law**

Clause 19 of the IP(A) Bill expands the scope of the legislation by amending the definition of telecommunications operator to encompass additional persons/companies involved in the provision of telecommunications services into the UK - including when they control or provide a telecommunication system located outside the UK.

The amendment reasserts UK government jurisdiction over entities established overseas under another jurisdiction, and holds one entity liable for the actions of another.

The definition of telecommunications operator was carefully enacted by Parliament during the passage of the IPA 2016, who considered the global nature of technology companies and the extra-territorial application of the legislation. 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.

The proposed reforms would undermine the principle established during the IPA 2016 passage stages, which set out that 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.

Therefore, we maintain strong concerns that, in the area of national security and law enforcement, departing from a jurisdictional nexus limited to the UK, infringes upon the sovereignty of other nations, their rule of law, and users' expectations in those countries not to be shaped by actions of a foreign government.

Furthermore, this will result in exacerbation of existing conflicts of law and could allow the UK government to require foreign companies to take actions that might conflict with their

own national laws. This will place private companies in an untenable position of facing an irreconcilable conflict of laws, for example from cybersecurity or privacy rules in both the UK and overseas.

Further complexity is added by the strict existing secrecy requirements, which prohibit operators that are under notice from disclosing the very existence of such notice. In practice, this could mean that when the requirements of a notice are in conflict with a domestic regulatory obligation or direction, a company is forced to break its domestic laws in order to comply with notice issued under the IPA. The company would not be able to communicate to the relevant government or regulatory authority the reasons for doing so, thus making it impossible to seek a diplomatic assistance to address the conflict. Administrative or civil enforcement may follow. In some cases (as with the UK's OSA and some overseas laws) there is also the possibility of criminal prosecution of company directors.

This proposed change marks a departure in the way the UK approaches the extraterritorial reach of UK law and consequential conflicts of law. While the Government recognised the extraterritorial reach and conflicts of laws created by the data acquisition powers in the 2016 Act, it also identified a partial solution in the form of the UK-US Agreement. However, currently the government has not set out any plans to work towards equivalent solutions.

Therefore, further clarity is urgently needed on how the proposed notice regime will operate in practice alongside potential conflicts arising from extraterritorial reach and enforcement, with clear mitigations for operators to preserve their freedom to operate in the UK and internationally.

(8 February 2024)