CCIA Submission

Investigatory Powers Act (Amendment) Bill Call for Evidence

About CCIA

CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest heavily in research and development, and contribute trillions of pounds in productivity to the global economy. This submission reflects analysis that CCIA has shared with interested MPs and Peers and is based on experience engaging with regulation of investigatory powers in a range of jurisdictions over decades.

Introduction

Without appropriate amendments, the new Bill to expand the Investigatory Powers Act would establish a system where the Home Office has a de facto veto on product development. It could block changes even if they are in the best interests of users, in theory to maintain access to data for law enforcement.

While responsible businesses are always ready to support legitimate law enforcement efforts, there has been a growing concern that the IPA might erode user privacy and weaken security. There have been long-standing worries about the potential for legislation to undermine privacy through end-to-end encrypted communications and enhanced user profiling or tracking.

Reducing security and data minimization efforts by creating backdoors to encrypted data or forcing companies to maintain redundant data would pose serious risks to the overall security and confidentiality of the public's communications and online accounts, be that people's communications, activity or location data; this seems inconsistent with existing legal protections for personal data. Weakened security ultimately leaves online systems more vulnerable to all types of attacks. You can't just build a backdoor for the "good guys" — once a vulnerability exists, it will be exploited.

Parliamentary process

This legislation was introduced in the Lords, which means there will be less opportunity to scrutinise and amend the bill after its passage through the Commons. There was an acknowledgement in the Lords that concerns around the Bill have not been fully investigated or addressed, with Lord Fox, for example noting that:

> *"[There] appears to be a gulf in both position and understanding between the Government and the tech companies, both on the principle of the notice and its details, which is, in a sense, frustrating scrutiny of the Bill. I understand that there is a*

> *disagreement about the introduction of notification notices in general. It is right that we look at the details to ensure that the process takes place in a way that reflects the realities of international law, and the need of the intelligence services to maintain levels of data access and the necessary safeguards.*
>
> *Concerns raised by stakeholders keep striking at the same places: how this notice would work with access agreements with other countries; why there is no double lock on the notification notice, despite the clear impact it would have on tech companies' activities; and why the definition of telecoms operator is perhaps in reality wider than the Government intend."*

This means that it is particularly important that the House of Commons is able to properly scrutinise this legislation, amends it appropriately and avoids unnecessary harms to the security of digital services, access for UK consumers to services they love, and the UK's reputation as a safe market in which to invest.

How would the IPA change?

Veto on product development

In the new legislation a combination of new notification notices and beefed up powers provide the Home Office an effective veto on changes to digital services around the world. These new powers are disproportionate and are raising concern in the UK and global tech sector. The new IPA framework would be difficult for companies to reconcile with the push from regulators and other friendly governments to increase data protection, minimise the amount of data collected and improve security. Security improvements, in particular, often need to move fast, responding to new threats. With the huge opportunities in AI we are seeing this should be a time to increase security — not weaken it. Cybersecurity experts in the United States have sounded the alarm about these UK proposals with Jim Baker and Richard Salgado writing:

> *"The proposal [...] runs counter to other efforts by numerous governments—including the U.K.—to urge the private sector to find better ways to substantially enhance cybersecurity on a more sustainable basis. Instead of doing that, the bill, as currently drafted, jeopardizes data security and privacy in pursuit of an understandable goal of helping law enforcement and intelligence agencies' legitimate objectives. But no one needs a law that could limit future progress on much-needed security enhancements, such as through the increased use of encryption. The bill needs to be fixed."*

Over time this will push tech firms to refocus product development away from addressing the priorities of UK consumers, towards government demands for access. The obstacles the new regime creates will be a drag on innovation and therefore undermine the quality of digital services on offer. They could risk deterring investment in improving services for UK consumers and contribute to a sense that the UK is not a safe market in which to invest. The most affected services could withdraw from the UK entirely.

International legal risk

These proposals have not been seen in other democratic countries. They go against principles of data minimisation that are enshrined in data legislation in many countries (including the UK) and could undermine all kinds of innovation. There is a real risk that companies will be caught between different regimes, when meeting UK requirements may result in breaching regulations in other friendly countries. techUK has noted that given the secrecy requirements in the Bill, companies may not be able to tell other governments why they are unable to comply with their requests and seek diplomatic assistance in resolving the issue.

Privacy protections

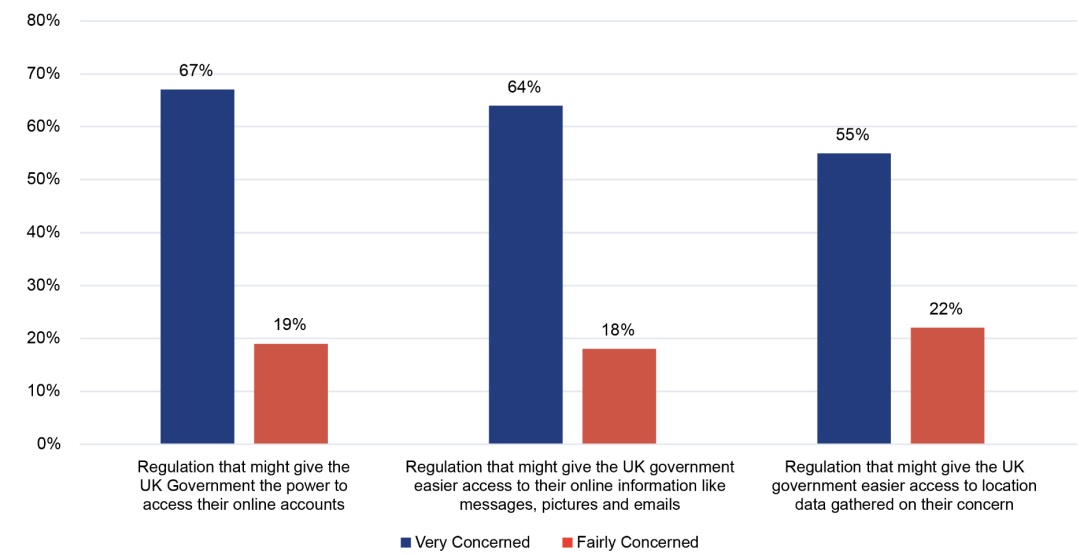
Revisions to the IPA weaken existing protections that are intended to ensure these powers are used appropriately. The new notifications notice would only require approval by the Home Secretary, not the existing "double lock" where it has to be approved by the Home Secretary and a Judicial Commissioner. There is good reason to believe that this does not reflect public priorities for services online, covered in the next section. This means their trust in digital services may be diminished with consequences for digital access and economic performance.

What do the public think?

ORB polling for CCIA suggests that a very broad spectrum of voters are concerned about the potential for intrusion into their private communications.

This is reflected in how people described their choices online, with 50% saying privacy, data minimisation and end-to-end encryption are an important factor when deciding which messaging service to use, for example.

FIGURE 1:
Voters are clearly concerned about the potential for intrusion into their private communications



Source: CCIA commissioned poll by ORB International

By contrast, levels of concern are notably more muted around justifications for a more intrusive regime. For example, 19% strongly agreed and 32% somewhat agreed with the proposition that internet companies should be required to share their data for law enforcement purposes such as police investigations. The comparison between the set of statements where people expressed strong concerns about regulatory requirements that might infringe their privacy, and the responses to questions about various justifications for the government to have access to that data is stark. It is hard to look at this data and not see a simple result: while people are supportive of effective engagement between internet companies and the government to address important goals like national security, they attach a higher priority to protecting their security and privacy.

What should happen next?

There are four priorities for the next steps for the Bill:

- **Give Parliament time to review the Bill.** TechUK recently published its concerns that serious changes are being presented as minor adjustments and may not see the scrutiny (and potential amendments) required. The same will be true for secondary legislation, where the Government should commit to give stakeholders time to respond to any public consultations on how the notices regime will operate.
- **Remove the risk of a veto on product changes.** The Notices requirement should be removed or at least include the same procedural protections as the "technical capability notice" (TCN) regime. The new law should not create an effective veto on product changes, which might stifle innovation and particularly urgent security improvements.

- **Address conflicts of law between the UK and other countries.** The new regime should not ignore issues of jurisdiction and corporate structure in issuing requests for data. This might include making it clear that the amendments are not meant to seek EU user data under the U.S.-UK Data Access Agreement and that companies will not be in breach because of meeting requirements in other friendly countries. More broadly, the Government should only enforce these provisions in the UK for UK users.
- **Include proper procedural safeguards.** Operators should not be required to comply with a notice before the full appeals process is complete. At a minimum there should be a statutory time limit for appeals to avoid an indefinite halt, this would build on the requirement for the Home Secretary to review notices within a specific time period that has been introduced to address this evident problem.