RESPONSE TO CONSULTATION

CCIA response to Consultation: Codes of Practice and Notices Regulations

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. Many of CCIA's members operate innovative, global digital services where consumers have high expectations for privacy and security, which means they might be affected by the constraints that notification notices could create for product changes.

Impact on innovation and privacy

If there is not a suitably clear timeline for a Home Office review of any changes, there will be the potential that companies providing digital services in the UK face an indefinite hold on their ability to make changes while a review process is ongoing (during which they are expected to maintain the "status quo" in terms of law enforcement access). Without some form of de minimis threshold this is likely to create uncertainty around all kinds of innovation and particularly important privacy and security changes that support trust in digital services.

Over time this will push tech firms to refocus product development away from addressing the priorities of UK consumers and businesses, 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. All of these impacts can be mitigated the more companies are satisfied that there is a process that will give them a realistic opportunity to engage with decision-making, a timeline for appropriate decisions to be made, and effective review.

International implications

This has international implications because the new IPA framework will 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 changes, in particular, often need to respond quickly to new global threats. The recent Salt Typhoon cyberespionage operation highlights the sophistication and scope of cybersecurity threats that digital services have to mitigate. Improvements responding to such evolving threats cannot be held up by cumbersome, unilateral UK requirements. Cybersecurity experts in the United States have sounded the alarm about the new UK law 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."*

Meredith Broadbent at the Center for Strategic and International Studies subsequently wrote:

> *Because Parliament acted in haste, there has not been sufficient recognition by the UK government that changes to the Investigatory Powers Act can be expected to magnify conflicts of law, dampen technological and security advancements in digital services, and raise issues of extraterritoriality and regulatory compatibility with trading partners, particularly the United States and Europe.*

There is a 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 Act, 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.

Opportunities to address these concerns in the guidance

Leaving aside wider changes to the regulation, there are opportunities in "the Guidance" (in this case, referring principally Annex H to the consultation) to mitigate industry concerns and smooth the process for the government.

- **De minimis thresholds:** reducing what could be an unmanageable volume of changes and reflecting commitments to Parliament that "patches" would not require notices.
- **Analytical requirements:** ensuring that the Secretary of State and Judicial Commissioner can consider impacts on innovation and privacy.
- **Appropriate advice on reasonable time:** using the analytical support available through the Technical Advisory Board to improve decision-making over a reasonable time.
- **Flexibility in review periods:** where firms feel a case is clear, giving them the option to request an expedited review could remove unnecessary obstacles to improvements.
- **Anticipating impacts on AI:** ensuring that data retention requirements are flexible enough for it to be practical to realise the Government's aspirations for UK AI development.
- **Allowing for engagement around conflicts in law:** creating opportunities to understand and mitigate conflicting requirements.

De minimis thresholds

The Guidance acknowledges that there is a scale at which the cost and disruption associated with some notices under this regime is not justified, e.g. for small companies (7.3) and for patches (14.12). There should be a broader de minimis threshold for notification notices to avoid a situation where complex global services have to issue a volume of notices that it will be impractical and unproductive for the Government to review. Companies that feel they are having to submit (or might have to submit) an unrealistic number of notification notices could be allowed to propose a set of thresholds to the Secretary of State, subject to review by the Judicial Commissioner as with other decisions under the Act.

The Government could also mitigate these concerns by constraining the categories for notification notices in the first place. The current scope of notification notice is so expansive that it is not compatible with the realities of product development. To address this the Government could, for example, restrict the potentially extremely broad category of "new functionality" to those in which there is a potential adverse impact on capability.

Analytical requirements

The matters to be considered by the Secretary of State in the Guidance allow for cost and a generic set of other impacts on the operator (4.21). It should more explicitly require a consideration of the most likely unintended consequences of a notification notice:

- Impacts on innovation: the Secretary of State should consider whether the proposed notice either directly, or by implication for other product changes, might inhibit innovation.
- Impacts on privacy: the Secretary of State should consider whether the proposed notice might inhibit privacy by reference to generally-accepted standards reflected, for example, in guidance to firms from the Information Commissioner's Office (ICO).

Appropriate advice on reasonable time

The Guidance anticipates a need to strike what may be a difficult balance between allowing the Secretary of State sufficient time and not overly impeding product changes (14.20). It states that it would be impractical to define this further but should anticipate how much a decision will be made in a fair and technically-appropriate manner, reflecting the characteristics of the relevant services. In the event of uncertainty or a disagreement over what constitutes "reasonable time", the Secretary of State should consult the Technical Advisory Board and share their analysis with the company to inform a resolution (as in 7.4).

The concept of reasonable time should also be extended to companies subject to notification notices, with a reasonable period in which to establish an appropriate compliance process.

Flexibility in review periods

While generally speaking it is more important for reviews to come to the right conclusion, there will be instances in which companies feel a case is relatively clear cut. In those instances,

there should be an option for companies to request an expedited review in a shorter period than 180 days (11.6). This should be reflected in the regulations.

Anticipating impacts on AI

The Guidance includes changes in data retention periods as a type of relevant change. This may produce particular challenges for AI services where the volume of data being processed, retained and then removed could materially affect overall costs. This could mean that notification notices create an unintended but significant barrier to the Government's aspiration (expressed elsewhere, e.g. in a recent consultation on copyright and AI) that AI developers can "train leading AI models in the UK". The Guidance should consider a need for these decisions to be made flexibly and quickly both in whether notification notices are given on AI development (14.15) and as a part of the review of any notice (13.4).

Allowing for engagement around conflicts in law

While some conflicts of law may be difficult to resolve, in many cases the impact may at least be mitigated by engagement with the relevant authorities responsible for enforcing conflicting laws. There is already an allowance in the Act for companies to disclose the existence and content of notices. The circumstances in which disclosure might be permitted (10.19) should include:

- UK regulators, particularly the Information Commissioner's Office.
- International law enforcement institutions, particularly the European Commission and the U.S. Department of Justice.

Companies should then be enabled to request to the Secretary of State that some form of dialogue with those organisations is undertaken to understand and if possible resolve potential conflicts.