24 February 2025

The Rt Hon Yvonne Cooper
Secretary of State for the Home Department
2 Marsham Street
London
SW1P 4DF4

The Rt Hon Sir Brian Leveson
Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU

RE: Request by Small Business Technology Developer Community for the Protection of End-to-End Encryption to Support the United Kingdom's Security and Economic Goals

ACT | The App Association is a trade association representing small business technology companies from across the United Kingdom (UK), European Union (EU), and the United States (U.S.). Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. **The App Association writes this open letter to strongly encourage the UK Home Office to withdraw its demand that Apple build a backdoor into its end-to-end encrypted services.**

Media reports suggest that the UK Government has issued a technical capability notice (TCN) under Section 253 of the Investigatory Powers Act 2016 compelling Apple to introduce a backdoor into its end-to-end encrypted cloud services. This would embed a systemic security vulnerability into the world's second-largest mobile device provider, endangering the security and privacy of all its users—not just in the UK, but worldwide. Additional reporting indicates that Apple has now discontinued its Advanced Data Protection feature in the UK, an optional service that offers end-to-end encryption for iCloud backups, file storage, and certain other apps.

The App Association's small business members both in and outside of the UK know that, in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorised users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorised users. End-to-end encryption is a primary tool for providing the trust and security of their customers. Attempts by governments—most recently the UK—to mandate backdoors to encryption algorithms significantly undermines these goals.

The App Association understands and appreciates the need for policymakers to protect public safety across new and emerging digital modalities. However, the TCN issued by the UK government to Apple does not accomplish this goal. Its implementation deeply damages security and trust across the digital economy by creating flaws in algorithms that can be used to compromise data confidentiality, integrity, and access requisites.

It is impossible to reserve security backdoors for just the 'good guys'. If a door exists then bad actors can, and will, exploit it. It is fair to assume that other tech firms will be asked to create similar backdoors into encrypted services, further damaging security and trust.

The UK's demand also sets a precedent for other countries and regimes to demand similar access to encrypted private data, further reducing citizens' privacy and safety.

The damage that would be caused by the implementation of the UK government's TCN is not hypothetical. As a prime example, government mandates in the 1990s for broadband internet providers to enable law enforcement agencies access to encrypted communications on their networks has directly led recently to the China-backed hacker group Salt Typhoon gaining unprecedented unauthorised access to swaths of sensitive data. While the magnitude of this breach of U.S. telecommunications carrier networks continues to be investigated, at this time it appears that Salt Typhoon's access was essentially unlimited. This (ongoing) episode is the strongest evidence that mandating unfettered access via backdoors to encrypted devices or data in transit will result in that access being exploited by unintended actors.

The Salt Typhoon experience demonstrates that weakening encryption will expose businesses to more frequent breaches, creating an even greater risk for those already marginalised.

The UK government's TCN also stands in stark contrast the UK government's own findings and priorities. Only a month ago, the UK's National Audit Office released a report detailing the dire threat posed by hackers to the UK government's operations and goals.[1] With cyber attacks to critical infrastructure continuing to increase in both frequency and severity, the need for security that end-to-end encryption provides has never been more essential. A mandated weakening of encryption will undermine the stated goal in the UK's 2022-2030 Government Cyber Security Strategy of 'protect[ing] and promot[ing] its interests as a sovereign nation in a world fundamentally shaped by technology'.[2]

In compelling a company to covertly compromise the security of its product, the UK government raises serious concerns about the security of products from UK firms, including our members who work to grow and create jobs in the UK, leading to investors and consumers questioning whether their products contain hidden security vulnerabilities mandated by the UK government. The precedent the TCN creates may also force some of our members to consider withdrawing from the UK market to avoid the reputational risks associated with undermining their own product's security. Lastly, the effective policy approach taken through issuing the TCN has, and will continue to, damage the UK's standing in global security and innovation policy,[3] and represents a ceding of leadership in this respect.

Government attempts to undermine encryption damage and distort security and competitiveness foundations in the UK market that our small business innovator community relies on. The UK has the power to protect encryption standards, ensuring they remain strong enough to safeguard our digital infrastructure without creating loopholes that compromise security. We call on the UK government to exercise this power in partnership with our community to reach a common goal – a secure and competitive UK digital economy.

---

[1] https://www.nao.org.uk/press-releases/cyber-threat-to-uk-government-is-severe-and-advancing-quickly-spending-watchdog-finds/.

[2] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

[3] Notably, the European Court of Human Rights (ECtHR) has condemned governments requiring companies to disclose encryption keys as disproportionate measures that breach human rights law. https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}.

Accordingly, we request that the UK government withdraw the TCN and engage in a revised policy development process to ensure that end-to-end encryption supports UK national and economic security. Our community fully commits to participating in such a process, and to more broadly support policies that enhance security and innovation as well as the UK's global leadership.

Sincerely,

Morgan Reed
President

Stephen Tulip
UK Country Manager

ACT | The App Association