February 26, 2025

The Honorable Pam Bondi
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue Northwest
Washington, District of Columbia 20530

The Honorable Kash Patel
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue Northwest
Washington, District of Columbia 20535

The Honorable Tulsi Gabbard
Director
Office of the Director of National Intelligence
1500 Tysons McLean Drive
McLean, Virginia 22102

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

Dear Attorney General Bondi, Director Patel, and Director Gabbard:

ACT | The App Association is a trade association representing small business technology companies from across the United States. 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 to strongly encourage your coordinated efforts to support U.S. security and competitiveness by opposing the United Kingdom's (UK's) Home Office 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 one of the world's largest mobile device providers, 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.
h
The App Association's small business members know that, in order to compete across consumer and enterprise markets, they must be able to reliably restrict data access to authorized users, ensure data remains accurate and unmodified, and guarantee information is available when needed by authorized 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 will deeply damage 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 to American small businesses innovating and competing across the global digital economy 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 unauthorized 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 marginalized.

The UK government's issuance of the reported TCN also stands in stark contrast the U.S. government's efforts to encourage the use of encryption for securing critical infrastructure, businesses, and personal data; promote best practices for encryption in cybersecurity; and for the U.S. government itself to use encryption to protect classified information and communications. 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

In a separate letter,[1] we have explained to the UK Home Office that in compelling a company to covertly compromise the security of its product, the UK undermines its own stated goal of "protect[ing] and promot[ing] its interests as a sovereign nation in a world fundamentally shaped by technology"[2] and raises serious concerns about the security of products from UK firms, leading to investors and consumers questioning whether their products contain hidden security vulnerabilities mandated by the UK government. The precedent the TCN implementation will create may 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, representing the closing off of a key market to countless U.S. small business innovators. Any government that mandates, or attempts to mandate, backdoors to encryption damages their own standing in global security and innovation policy.

We strongly support your efforts to combat other governments' attempts to undermine encryption damage and distort security and competitiveness foundations that our small business innovator community relies on. The United States has the power to protect encryption standards, ensuring they remain strong enough to safeguard our digital infrastructure without creating loopholes that compromise security. We request your leadership in pushing back

[1] https://actonline.org/wp-content/uploads/ACT-Ltr-re-UK-Encryption-TCN-24-Feb-2025.pdf.
[2] https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

against the UK Home Office's reported TCN, and for your partnership in engaging the UK government (and other governments around the world) in a new policy dialogue to ensure that end-to-end encryption supports U.S. 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 U.S.' global leadership.

Sincerely,

Morgan Reed

President
ACT | The App Association