

March 13, 2025

The Honorable Pamela J. Bondi
Attorney General
U.S. Department of Justice

The Honorable Howard W. Lutnick
Secretary of Commerce
U.S. Department of Commerce

The Honorable Kristi Lynn Noem
Secretary of Homeland Security
U.S. Department of Homeland Security

The Honorable Tulsi Gabbard
Director of National Intelligence
Office of the Director of National Intelligence

The Honorable Jamieson L. Greer
U.S. Trade Representative
Office of the U.S. Trade Representative

Re: Threats to Global Encryption in the UK

Dear General Bondi, Secretary Lutnick, Secretary Noem, Director Gabbard, and Ambassador Greer:

On behalf of the undersigned organizations, we write to express concern about the United Kingdom's reported use of the Investigatory Powers Act (IPA) to demand access to users' end-to-end encrypted material held in the Apple iCloud. We seek your assistance in raising concerns with the UK government about the significant consequences of this action.

We understand from news reports that the request from the UK government would have extraterritorial reach and require Apple to modify its iCloud system to create a backdoor for iCloud users worldwide. The implications of this move extend far beyond Apple, as the IPA gives the UK government power (under UK law) to seek not only personal communications, but also corporate communications held by any company that does business in the UK. We believe this move is both ill-advised and dangerous.

There is no such thing as an encryption backdoor that can only be used for good actors. The UK's policy will give bad actors and meddlesome regimes an opening to infiltrate private communications, business data and consumer information. Particularly in the wake of the Salt Typhoon hack, we need governments to stand for policies that make information more – not less – secure.

The consequences of the UK's ill-advised choice will be felt directly by U.S. companies and consumers. Ultimately, these changes will severely harm technological development both within and outside the UK, negatively impact consumer rights and freedoms, and catastrophically weaken global safety and security.

Requiring non-UK-based companies to comply with changes that would affect their products globally, particularly access to sensitive consumer information that Apple itself cannot view, would dissuade a host of societally beneficial technological developments. The move will necessarily force companies to avoid offering truly encrypted products and services to their customers located in the UK – which Apple has already announced – *and* weaken encryption protections for their global customers, including those within the United States.

The decision will also spell disaster for U.S. citizens' privacy and security. State surveillance creates a chilling effect and undermines free expression by removing a tool used by U.S. speakers both within and outside the UK. Weakening encryption will leave US citizens more vulnerable to spyware and other surveillance tools employed by bad actors globally, as well as "snooping" by unscrupulous private parties. It will also empower authoritarian regimes to stifle dissent, compel action by U.S.-based companies, and undermine U.S. economic and national security interests.

While we recognize and support the legitimate needs of law enforcement to take advantage of every practical and ethical tool at its disposal to pursue bad actors, creating a backdoor and weakening encryption will lead to grave consequences for cybersecurity, innovation, and privacy.

We appreciate the steps the Trump Administration has taken to engage the UK government about this troubling development. While we are hopeful those efforts will lead to a resolution, we remain concerned by the broad scope of the IPA and its implications for the UK's status as a qualifying nation under the CLOUD Act. We

respectfully request an opportunity to meet with you or your staff to discuss this matter further.

We appreciate your leadership in standing up for the interests of U.S. companies. We look forward to engaging with you on this important issue.

Sincerely,

Software & Information Industry Association (SIIA)
ACT | The App Association
Computer & Communications Industry Association (CCIA)
Consumer Technology Association (CTA)
TechNet

cc: The Honorable Michael G. Waltz, Assistant to the President for National Security Affairs

The Honorable Kevin A. Hassett, Assistant to the President and Director, National Economic Council