February 21, 2025

The Honorable Marco Rubio
Secretary of State
U.S. Department of State
2201 C Street NW
Washington, DC 20520

The Honorable Pamela Bondi
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington DC 20530

The Honorable Jeremy Pelter
Acting Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

The Honorable Michael Kratsios
Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20530

Re: UK demands access to encrypted data worldwide

Dear Secretary Rubio, Attorney General Bondi, Acting Secretary Pelter, and Director Kratsios,

We write to urge you to take immediate action to protect Americans' digital speech and data from the United Kingdom's Home Office efforts to break secure encryption. Every American has "the right to be free from state inquiry into the contents of his library."[1] Acting under the UK Investigatory Powers Act of 2016, the UK's Home Office has sent "technical capability notices" to Apple reportedly demanding access to "all the content any Apple user worldwide has uploaded to the cloud"[2]—including tens of millions of Americans. This demand has "no known precedent in major democracies."[3] It compels Apple to decrypt, and allow the UK access to, user data currently protected by end-to-end encryption (E2EE), the best available technology for protecting stored messages, documents, and other material. The Home Office's notices require immediate compliance even pending an appeal through a process that is—like the notices—secret by law.

While Congress should enact a law prohibiting American tech companies from providing encryption backdoors to any country[4], barring swift congressional action, the federal government should use all leverage at its disposal to convince the UK Home Office to change course. In particular,

---

[1] Stanley v. Georgia, 394 U.S. 557, 565 (1969).

[2] Joseph Menn, *UK orders Apple to let it spy on users' encrypted accounts*, Wash. Post (Feb. 7, 2025), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/. Because these notices are required to be secret, similar demands may also have been made to other companies. Apple's Advanced Data Protection is optional for iCloud users.

[3] *Id.*

[4] This would create a 'conflict of laws' situation, allowing Apple to fight this order in UK courts and protect Americans' safety and security.

the United States could threaten to terminate the UK-US Cloud Act agreement of 2019[5] if the UK does not withdraw its demands to Apple. This agreement has been of considerably greater value to the UK than to the US and it is already past its original five-year term and is ripe for reconsideration anyway.

The UK's demand puts users at risk. To comply, Apple must either build a backdoor into its end-to-end encrypted cloud service (which could, and would, then be accessed by malicious actors) or cease offering E2EE cloud services altogether. Either way, it appears that Apple would have to make such changes not only for users within the UK but worldwide. Apple is right: no single government should "have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption."[6]

Of course, the UK is not constrained by our Constitution but, by demanding access to encrypted cloud storage for users *worldwide*, the UK is nonetheless vitiating Americans' Fourth Amendment rights to be secure in our "papers and effects" and First Amendment rights "to receive information and ideas."[7] This right means nothing unless Americans' private information is secure. Government snooping chills speech—it discourages those who, "motivated by fear of economic of official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of [their] privacy as possible,"[8] must keep their thoughts and communication secure from prying eyes.

"The door barring federal and state intrusion into" Americans' privacy of information "cannot be left ajar; it must be kept tightly closed[.]"[9] Breaking end-to-end encryption for one cause will lead ineluctably to "encroachment upon more important interests."[10] Our present moment perfectly illustrates the point: through its Salt Typhoon hacking operation, the Chinese Communist Party is throwing this right to security of information into doubt.[11] Salt Typhoon has compromised at least nine telecom firms—apparently by accessing our governments' own backdoors into telecom networks. If the UK government's action is left to stand, without a swift and effective American response, the result will be the creation of more backdoors for the CCP and other adversarial nations to exploit.

---

[5] Dep't of Just., Cloud Act Agreement between the Governments of the U.S., United Kingdom of Great Britain and Northern Ireland (Oct. 3, 2019), https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern.

[6] Menn, *supra* note 2.

[7] Stanley v. Georgia, 394 U.S. 557, 564 (1969).

[8] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341-42 (1995).

[9] *Stanley*, 394 U.S. at 563 (quoting Roth v. United States, 354 U.S. 476, 488 (1957)).

[10] *Id.*

[11] *See* Fed. Commc'ns Comm., Fact Sheet: Implications of Salt Typhoon Attack and FCC Response (Dec. 5, 2024), https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf.

The UK's decision to go after Apple, in particular, seems designed to send a message. Apple is renowned for its cybersecurity and data protection. If the UK can force Apple to expose its users' stored data, it can force any cloud storage provider to do so. If the UK is not made to back down now, this will only be the beginning. If the UK has its way, when the next Salt Typhoon comes along, Americans will have no end-to-end encrypted services in which to seek shelter from government surveillance. In a borderless world, our Fourth and First Amendment rights will be meaningless.

Ultimately, the UK's demands are unlikely to withstand judicial review even under the weaker protection of European fundamental rights law, as the attached letter explains. But you cannot wait for the European Court of Human Rights to act. The UK's notice was already served in January and requires immediate compliance even during an appeal, which Apple has likely already undertaken but which is secret by law. We urge you to act swiftly to protect Americans, and Internet users everywhere, from having their stored communications exposed to access by malicious governments and non-state actors.

Sincerely,

Civil Society Organizations

TechFreedom
Advocacy for Principled Action In Government
American Consumer Institute
Competitive Enterprise Institute
Freedom of the Press Foundation
New America's Open Technology Institute
R Street Institute
The Future of Free Speech

Academics & Computer Scientists[12]

Neil Chilson
Head of AI Policy
Abundance Institute

Jess Miers
Visiting Assistant Professor of Law
University of Akron School of Law

Brian L. Frye
Spears-Gilbert Professor of Law
University of Kentucky College of Law

Riana Pfefferkorn
Policy Fellow
Stanford HAI

cc: The Honorable John Thune, U.S. Senate Majority Leader
The Honorable Charles Schumer, U.S. Senate Minority Leader
The Honorable Mike Johnson, Speaker of the U.S. House of Representatives
The Honorable Hakeem Jeffries, U.S. House Minority Leader

[12] Individual signatories' affiliations are shown for purposes of identification only.