UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chairman

Dear [Company CEO/Executive]:

Americans rightly hold dear the First Amendment and its guarantee of freedom of speech. We understand that America's greatness and prosperity stems in no small part from its zealous commitment to the free exchange of ideas.[1] We know, as sixteen-year-old Benjamin Franklin knew when he wrote in *The New-England Courant*, using the persona of a middle-aged widow named Silence Dogood, that "[w]ithout freedom of thought, there can be no such thing as wisdom; and no such thing as public liberty, without freedom of speech...."[2] In the 21st century, the public squares in which citizens gather to exchange ideas and engage in lively debate now include online platforms.[3] Because online platforms have become so critical to public discourse, pervasive online censorship in recent years has outraged the American people. Not only have Americans been censored and expelled from platforms for uttering opinions and beliefs that were not shared by a small Silicon Valley elite, the previous administration actively worked to encourage such censorship.[4]

President Trump has put a swift end to the weaponization of the federal government against Americans and their freedoms,[5] but foreign governments present emerging and ongoing threats to the free exchange of ideas.[6] Companies might be censoring Americans in response to the laws, demands, or expected demands of foreign powers. And the anti-encryption policies of foreign governments might be causing companies to weaken data security measures and other technological means for Americans to vindicate their right to anonymous and private speech. Specifically, there have been numerous recent attempts by foreign governments to pressure your company to censor content or degrade security for users of your services. Examples of these efforts

---

[1] As James Madison observed, a critical role of government is to protect the "diversity in the faculties of men." The Federalist No. 10, at 58 (James Madison) (Jacob E. Cooke ed., 1961).
[2] Silence Dogood No. 8, The New England Courant (Jul. 9, 1722), https://founders.archives.gov/documents/Franklin/01-01-02-0015.
[3] *See Packingham v. North Carolina*, 582 U.S. 98, 104 (2017) (describing "the vast democratic forums of the internet in general, and social media in particular," as "the most important places . . . for the exchange of views" (cleaned up)).
[4] Committee on the Judiciary of the U.S. House of Representatives, Select Subcommittee on the Weaponization of the Federal Government, *Final Staff Report: The Weaponization of the Federal Government* (Dec. 20, 2024), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2024-12/Part-1-Final-Weaponization-Report-Compilation.pdf.
[5] Exec. Order No. 14149, 90 Fed. Reg. 8243, Restoring Freedom of Speech and Ending Federal Censorship (Jan. 20, 2025).
[6] *See generally* Sean Moran, *Jim Jordan's 'Censorship Files': UK Government Tried to Censor Criticism of Mass Migration, 'Two-Tier' Policing*, Breitbart (July 31, 2025) (describing Congressional investigation as revealing how UK was telling platforms to censor true narratives about a two-tier justice system), https://www.breitbart.com/tech/2025/07/31/jim-jordan-uk-government-tried-to-censor-criticism-of-mass-migration-asylum-refugees/.

include the European Union's Digital Services Act (DSA),[7] which "incentiviz[es] tech companies to censor speech, including speech outside of Europe";[8] the United Kingdom's Online Safety Act,[9] which requires online platforms to "protect" their users from harm by detecting and removing "illegal content;" and reported demands from the UK's government under its Investigatory Powers Act[10] that companies weaken their encryption measures to enable UK law enforcement to access data stored by users.[11]

I am concerned that these actions by foreign powers to impose censorship and weaken end-to-end encryption will erode Americans' freedoms and subject them to myriad harms, such as surveillance by foreign governments and an increased risk of identity theft and fraud. I am also concerned that companies such as your own might attempt to simplify compliance with the laws, demands, or expected demands of foreign governments by censoring Americans or subjecting them to increased foreign surveillance even when the foreign government's requests do not technically require that. Indeed, foreign governments seeking to limit free expression or weaken data security in the United States might count on the fact that companies have an incentive to simplify their operations and legal compliance measures by applying uniform policies across jurisdictions.

As you grapple with how your company will comply with these misguided international regulatory requirements, I write to remind you that your company has independent obligations to American consumers under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.[12] As the nation's consumer protection agency, the FTC has taken action for over two decades against companies that fail to keep their data security or privacy promises to consumers.[13] The Commission has steadfastly maintained that companies that collect, use, share, or transmit consumers' personal data must employ reasonable

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) (hereinafter "Digital Services Act").
[8] Committee on the Judiciary of the U.S. House of Representatives, Interim Staff Report, *The Foreign Censorship Threat: How the European Union's Digital Services Act Compels Global Censorship and Infringes on American Free Speech* at 2 (Jul. 25, 2025), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/2025-07/DSA_Report%26Appendix%2807.25.25%29.pdf.
[9] https://www.legislation.gov.uk/ukpga/2023/50.
[10] https://www.legislation.gov.uk/ukpga/2016/25.
[11] *See* Zoe Kleinman, *UK demands access to Apple users' encrypted data*, BBC (Feb. 7, 2025), https://www.bbc.com/news/articles/c20g288yldko; Joseph Menn, *U.K. 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/.
[12] 15 U.S.C. § 45(a).
[13] *See* FTC Press Release, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case* (Aug. 13, 1998), https://www.ftc.gov/news-events/news/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting-personal-information-agencys-first; FTC Press Release, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises* (Aug. 8, 2002), https://www.ftc.gov/news-events/news/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy-promises.

security measures, including encryption of sensitive information, to protect such information from unauthorized access, use, or disclosure.[14]

Companies that promise that their service is secure or encrypted, but fail to use end-to-end encryption where appropriate, might deceive consumers who reasonably expect that level of confidentiality. Further, certain circumstances may require reasonable security measures such as end-to-end encryption, and the failure to implement such measures might constitute an unfair practice.

Weakening encryption or other security measures to comply with the laws, demands, or expected demands of a foreign government may also violate Section 5. If a company promises consumers that it encrypts or otherwise keeps secure online communications but adopts weaker security due to the actions of a foreign government, such conduct may deceive consumers who rightfully expect effective security, not the increased susceptibility to breach or intercept desired by a foreign power.[15] Consumers may be further deceived if companies fail to prominently disclose that weaker security measures were adopted due to the actions of a foreign government, information that might be material to a consumer's decision to use a service. It might also be an unfair practice to weaken the security of Americans' communications to placate foreign powers that do not have Americans' best interests at heart and that might seek to surveil or otherwise hurt Americans.

Censoring Americans to comply with a foreign power's laws, demands, or expected demands can also violate Section 5. American consumers do not reasonably expect to be censored to appease a foreign power and may be deceived by such actions. And as with weakened security measures, consumers might be further deceived if companies do not prominently disclose that censorious policies were adopted due to the actions of a foreign government, as consumers might not want to use a service that exposes them to censorship by foreign powers. Further, it might be an unfair practice to subject American consumers to censorship by a foreign power by applying foreign legal requirements, demands, or expected demands to consumers outside of that foreign jurisdiction.

Protecting the privacy and security of Americans' personal data and safeguarding their liberty by combatting illegal censorship are priorities for the Trump-Vance FTC. Part and parcel of the Commission's efforts is engagement with stakeholders on these important issues. I invite you to reach out by Thursday, August 28th to schedule a time to meet with my office to discuss

---

[14] *Cf.* Thomas B. Pahl, *Stick with Security: Store sensitive personal information securely and protect it during transmission*, FTC Business Blog (Aug. 18, 2017), https://www.ftc.gov/business-guidance/blog/2017/08/stick-security-store-sensitive-personal-information-securely-and-protect-it-during-transmission; *FTC v. Ring, LLC*, No. 2023113 (D.D.C. 2003) (alleging that failure to encrypt videos of consumers in private spaces of home, among other security failures, was unfair); *Chegg, Inc.*, FTC No. 2023151 (2022) (same, as to personal information); *BJ's Wholesale Club, Inc.*, FTC No. 0423160 (2005) (same, as to credit card information).

[15] *Cf. Zoom Comms. Inc.*, FTC No. 1923167 (2021) (alleging that Zoom misled users by promising "end-to-end, 256-bit encryption" to secure users' communications, when in fact it provided a lower level of security); *Henry Schein Practice Solutions, Inc.*, FTC No. 1423161 (2016) (alleging that provider of office management software deceived dental practices about offering industry-standard encryption of sensitive patient information); *FTC v. Rennert*, No. CV-S-00-0861-JBR (D. Nev. 2000) (alleging that medical prescription website deceived consumers about website encryption).

how, in the face of competing pressures from global regulators, you will honor your privacy and security commitments to American consumers and meet your ongoing obligations under U.S. law.

Sincerely,

Andrew N. Ferguson
Chairman
Federal Trade Commission