Skadden

Cybersecurity and Data Privacy Update

September 4, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

FTC Chair Warns Tech Firms: Weakening Encryption or Censoring Americans for Foreign Governments May Violate US Law

Executive Summary

- **What is new:** On August 21, 2025, the chairman of the Federal Trade Commission (FTC), Andrew Ferguson, issued letters to more than a dozen technology companies warning that weakening encryption or censoring Americans in order to comply with foreign laws may violate Section 5 of the FTC Act.
- **Why it matters:** The FTC letters noted that applying policies designed to comply with foreign laws, such as the EU's Digital Services Act, to U.S. users could constitute unfair or deceptive practices under the FTC Act. The FTC emphasized that companies must honor their data security and free expression commitments to U.S. consumers, even when facing global regulatory pressures.
- **What to do next:** Companies subject to FTC jurisdiction should exercise caution before applying uniform global content moderation and data security policies to U.S. consumers, and should review statements to consumers to assess alignment with company practices.

Key Points From the FTC Letter

The FTC's letters highlight the commission's concern that tech companies may adopt content moderation or data security policies that, while designed to meet foreign legal requirements, could impermissibly infringe upon U.S. consumers' privacy, data security and free expression. Chairman Ferguson stated in the letters that Americans are increasingly subject to online censorship and weakening of security measures not only from domestic pressures, but also from the demands of foreign governments that exert influence over U.S. technology companies. The letters represent a new front in the ongoing conflict between the U.S. and European governments over the scope of European regulation of U.S. technology companies, which according to the U.S. administration includes arbitrary and discriminatory "digital taxes."

According to the FTC, technology companies may be censoring Americans in response to foreign legal requirements, and anti-encryption policies of foreign governments may lead companies to weaken their data security measures. The FTC expressed concern that technology companies may seek to simplify compliance with foreign laws, such as the EU Digital Services Act, the U.K. Online Safety Act and the U.K. Investigatory Powers Act, by adopting globally applicable content moderation and security policies that may lead to Americans experiencing increased censorship or increased susceptibility to foreign surveillance.

FTC Chair Warns Tech Firms: Weakening Encryption or Censoring Americans for Foreign Governments May Violate US Law

Chairman Ferguson stated that as companies develop compliance programs to address foreign laws, they should also consider the independent obligations they may have to U.S. consumers under Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices. Chairman Ferguson noted that the FTC has maintained that companies processing Americans' personal data must employ reasonable security measures (which may include encryption) to protect U.S. personal data from unauthorized access, use and disclosure.

Encryption

The FTC stated that companies that represent their services as "secure" or "encrypted" but fail to adopt end-to-end encryption where appropriate may deceive consumers who expect such security. In certain circumstances, the FTC explained, end-to-end encryption may be required as a reasonable security measure, and failure to provide it could also amount to an unfair practice under Section 5 of the FTC Act.

The FTC emphasized that what may be considered an unfair or deceptive act or practice does not change when the act or practice is intended to comply with foreign government legal demands or requirements — for example, the U.K. Investigatory Powers Act or EU's proposed Regulation to Prevent and Combat Child Sexual Abuse. Chairman Ferguson stated that weakening represented security measures in response to foreign legal demands may constitute deceptive conduct under the FTC Act. The FTC also cautioned that it may be an unfair practice to weaken the security of Americans' communications in response to foreign governments that may seek to surveil or harm Americans.

Censorship

Alleged censorship of American users to satisfy foreign legal regimes may also present risk under the FTC Act. The FTC stated that U.S. consumers do not reasonably expect to be censored by technology companies to accommodate the requirements of foreign governments and that doing so may be deceptive under Section 5 of the FTC Act. Chairman Ferguson explained that U.S. consumers may be further deceived if companies implement foreign-driven content moderation rules in the United States without prominently disclosing the basis for those changes — such as compliance with the EU Digital Services Act or U.K. Online Safety Act. Additionally, the FTC suggested that adopting uniform global policies that impose foreign censorship standards on American users outside of the foreign jurisdiction, particularly when not legally required, could itself be treated as an unfair practice.

What To Do Now

As the FTC letter makes clear, technology companies operating in the U.S. and Europe face competing and contradictory global regulatory requirements for content moderation and encryption.

In light of this, companies should exercise caution before adopting uniform content moderation or data security practices worldwide. While such strategies may reduce regulatory compliance burdens, the FTC's letters suggest that doing so may risk exposing a company to FTC investigation and potential enforcement actions. Companies therefore need to undertake a careful balancing act between U.S. and European compliance. Such balancing should include evaluation of content moderation and data security practices against both U.S. and EU legal requirements and expectations.

In particular, companies should:

- Evaluate (i) content moderation and data security policies that address compliance with foreign laws and (ii) policies related to responses to voluntary government requests to assess how such policies may impact American consumers.
- To the extent foreign requirements are driving changes in content moderation policies or security measures, disclose to U.S. consumers that such actions have been taken due to the actions of a foreign government (and consider any restrictions under those foreign laws that prohibit such disclosure).
- Review statements to consumers to confirm that privacy and data security representations, particularly regarding encryption and censorship, align with company practices.

FTC Chair Warns Tech Firms: Weakening Encryption or Censoring Americans for Foreign Governments May Violate US Law

Contacts

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Nicola Kerr-Shaw
Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Susanne Werry
Counsel / Frankfurt
49.69.74220.133
susanne.werry@skadden.com

Aleksander J. Aleksiev
Associate / London
44.20.7519.7000
aleksander.aleksiev@skadden.com

Dana E. Holmstrand
Associate / Washington, D.C.
202.371.7014
dana.holmstrand@skadden.com