

The Adversarial Platform Prevention (APP) Act

Senator Marco Rubio (R-FL)

The APP Act introduces a set of data protection and censorship related standards and restrictions that must be met by high-risk foreign software in order to legally operate in the United States.

The APP Act would define high-risk foreign software as any software owned by an entity organized under the laws of, headquartered in, or whose principal operations are in China, Russia, Venezuela, Cuba, or a country designated as a state sponsor of terrorism, or any software that stores U.S. consumer data in one of those nations.

- 1. Warning label on covered high-risk foreign software:** no covered foreign software may be made available without a warning label, which provides consumers information related to data and security risks of the software, as well as the ability to cancel the download.
 - a. The warning label must be separate from other disclosures and terms of service and must provide users with the option to cancel the download.
 - b. The warning must provide information related to the software's ownership, country of origin, associated data privacy risks, and whether the developer or owner of the software has ever provided consumer data to any law enforcement agency, intelligence agency, or other government entity of a covered country.

- 2. Disclosure related to covered high-risk foreign software:** Companies that own a covered foreign software are required to make an annual disclosure to the FTC and DOJ, which will be made publicly available, that includes the following:
 - a. The type of data of United States consumers being accessed;
 - b. A description of how the data is used by the owner;
 - c. A description of any consumer data protection measure in place that protects the rights and interests of United States consumers;
 - d. Internal content moderation policies related to U.S. and international consumers.

- 3. U.S. consumer data protections, disclosures and restrictions:** In an instance where the owner of covered foreign software receives requests from a law enforcement agency, intelligence agency, or other government entity of a covered country for data on U.S. persons, to censor U.S. persons, or to access the internal networks of the software owner:
 - a. The owner of a covered foreign software must disclose such requests to the FTC and DOJ within 14 days.
 - b. If the owner of the covered software has complied with the request, it is prohibited from making the covered software available in the U.S.
 - c. Requires the FTC and DOJ to issue regulations requiring an owner of covered foreign software to implement consumer data protection measures to ensure that any parent company in a covered country may not access the consumer data collected and stored, or otherwise held, by a subsidiary in the United States.

- 4. Additional prohibitions related to U.S. consumer data:** Any data collected on U.S. persons must be stored in the United States. Owners of covered foreign software are prohibited from selling any data collected on U.S. persons.

5. **Recourse for censorship:** The owner of a covered software is required to offer a means of appeal for any case in which an owner of covered foreign software censors the online activity of a person in the United States
6. **Nonapplication of Communications Decency Act protections:** Section 230 protections do not apply to covered high-risk foreign software.
7. **Investment screening:** Reflects the reality that malign actors can weaponize large quantities of commercially available, non-sensitive data by amending the current statute to include any U.S. firm that “maintains or collects sensitive **or commercially available** personal data of United States citizens that may be exploited in a manner that threatens national security,” as a criterion for CFIUS review.
8. **Federal preemption:** The APP Act includes an explicit preemption of state and local laws and regulations.

The legislation further establishes corporate and individual criminal offenses, requires a report to Congress, and creates the process for new and revoked designation as a covered country.