Free markets. Real solutions.

EXPLAINER

S.2033: American Innovation and Choice Online Act (AICOA)

Cybersecurity Legislative Analysis Series

Purpose: Makes covered platforms' preferential treatment of their own products and services unlawful.

Status: Referred to the Senate Judiciary Committee.

Rating: CYBER CONCERNS This bill has the potential to reduce the security of covered platforms drastically and either exacerbate or introduce cybersecurity vulnerabilities.

Last updated: Aug. 1, 2023 — Review Status

Key Provisions

- Regulates a subset of digital service providers by making preferential treatment of their own products and services unlawful.
- Outlines 10 categories of unlawful preferential treatment, to include:
  - Actions that would "materially harm competition," such as: preferencing their own products or services over those of other business users of their platforms; limiting the ability of business users' products or services to compete with the platform's own offerings; and discriminating in the application of their terms of service among similarly situated business users;
  - Materially restricting, impeding or unreasonably delaying efforts to access or interoperate with the covered platform's technology stack; and
  - Materially restricting or impeding a competitor from accessing data generated on or from the covered platform's products or services.
- Provides affirmative defenses, including for platform core functionality concerns, complying with state and federal laws, and protecting user privacy and platform security.

Background

In 2020, the House Judiciary Committee unveiled a 450-page report detailing alleged anti-competitive conduct by select companies. In an attempt to remedy this finding, legislators introduced the AICOA in both the House and Senate in 2021 (with revisions in 2022). According to sponsors, the bill aims to facilitate competition against tech companies and provide greater consumer choice. The AICOA sparked fierce debate among legislators, industry and advocacy organizations and, as a result, had not progressed to either chamber floor. Sen. Amy Klobuchar (D-Minn.), Sen. Chuck Grassley (R-Iowa) and several colleagues reintroduced the AICOA (S.2033) in June 2023.

As R Street's Cybersecurity team has written previously, the AICOA would raise significant cybersecurity and data privacy concerns. It has the potential to reduce the security of platforms drastically and either exacerbate or introduce cybersecurity vulnerabilities. (Other concerns exist, though we limited our scope here to cyber concerns.) Various cybersecurity and national security leaders have raised similar concerns. To improve the cyber considerations of this bill, legislators should consider removing or revising language to ensure the security of online platforms, any entities that may meaningfully interact with these platforms, and U.S. consumers.

Key Takeaways

This bill would have a number of chilling effects on cybersecurity, including:

- Introducing cyber vulnerabilities and risk of data compromise by requiring interoperability and/or data access across platforms and services through actions such as: (1) sharing sensitive or non-public data with competitors (and potentially malicious actors) that may not have adequate cybersecurity or privacy safeguards; or (2) allowing the installation of insecure software or hardware.
- Failing to specify whether platform users can apply any data sharing preferences to every service or application that interoperates or interacts with the covered platform.
- Risking damage to U.S. consumer trust and cyber safety in the event of a material cyber incident resulting from the above legal requirements.

Free markets. Real solutions.

EXPLAINER

S.2033: American Innovation and Choice Online Act (AICOA)

Cybersecurity Legislative Analysis Series

Cybersecurity Analysis

FACTORS	ANALYSIS
Access provisions	This bill would make unlawful any covered platform's material restriction or limitation of access of data to competitor platforms and services. The 2023 AICOA did carve an exception for interoperability of products and services offered in cases of "significant cybersecurity risk." The definition of what would qualify, as well as how a company would prove such a risk, is unclear. Companies would be on the defense to justify actions taken in the name of security.
Applicability	Given the global prominence and usage of covered platforms, this bill could affect consumers and businesses globally, though enforcement would only apply to the platform's U.S.-based presence—which may result in complicating or contradicting a covered platform's operations in global markets.
Business impact	Companies would incur costs to alter their business operations to adhere to the bill's provisions (or if they are found to be in violation of them). Forcing interoperability would impose costs on tech companies that must accommodate competing products and services. There may also be a dampening effect of investment in covered platforms if their innovations must be shared or interoperable with competitors. There is a chance that less efficient or malicious platforms would benefit. The influx of products and services would inevitably introduce a fair amount of cybersecurity and data privacy risks. While the bill would allow for affirmative defenses, platforms would bear the burden of establishing their applicability after the fact.
Accounts for different entities	This bill would focus solely on large tech corporations with 50 million monthly active users (or 100,000 monthly business users), as well as annual sales and market capitalization thresholds, that are considered "critical trading partners." The federal government can also designate online platforms as being covered.
Data privacy and security	Privacy and security concerns are significant. Cybercriminals and other malicious actors could take advantage of the bill's interoperability or data access clauses to either access sensitive information or install intentionally insecure products. While the bill excludes business users that pose "clear national security risk" or are associated with a foreign adversary's government, it would impose a large administrative burden on both enforcement authorities and covered platforms to consistently prove they pose such a risk. Furthermore, lists of malicious entities maintained by the federal government may not be comprehensive or up to date. Finally, there is a risk that adversaries may have already gotten what they needed by the time a threat is proven. For example, should a company remove its security requirements for listing applications on an app store, a host of unsecure or scam apps could be available for download. Furthermore, companies have argued that app store requirements allow users to control the amount of data they share with developers.
Rulemaking or update mechanisms	The Federal Trade Commission (FTC) and the Department of Justice (DOJ) would promulgate regulations to determine the implementation and enforcement of this bill.
Exemptions, exceptions and defenses	Safety and privacy are affirmative defenses, but the platform would bear the burden of asserting the affirmative defense. In the meantime, platforms would be culpable for violating the law, even if it was done in the name of security. Only two provisions provide an exception for security at the outset. A provision was added that allows for an exception to access or interoperability should that access create "significant cybersecurity risk."

FACTORS	ANALYSIS
Enforcement mechanisms	The FTC, DOJ and state attorneys general would be the primary enforcement mechanisms.
Other	It is unclear whether foreign or other domestic competitors would be subject to the same standards of conduct that "covered platforms" are, but this in and of itself would be concerning.

Recommendations

Alongside the cybersecurity and privacy concerns highlighted in our analysis, we put forth the following recommendations with the goal of reducing these risks.

SECTION AND SUMMARY	RECOMMENDATION(S)
Unlawful Conduct Section 3(a)(4) Platform interoperability	**Remove this provision.** Forcing interoperability across numerous platforms and services without a clear definition of what interoperability entails has the potential to be costly and create cyber vulnerabilities. While the text carved out an exception for "significant cyber risk," it is unclear how covered platforms would prove cyber risk without potential disclosure of sensitive or otherwise non-public data. This could impact a company's ability to protect sensitive or other non-public data from malicious actors who would take advantage of relaxed privacy and security controls.
Unlawful Conduct Section 3(a)(7) Data access	**Remove this provision.** This provision would expand business user access and could jeopardize data security if the business user is an unverified third party that does not employ adequate safeguards.
Unlawful Conduct Section 3(a)(8 Uninstalling preinstalled apps or changing default settings	**Amend this provision to exclude security applications or processes from the restrictions for user freedom of choice on platforms;** **Amend provisions to unlawful conduct to include security exemptions *or* make a standalone security provision applicable to all; and** **Amend the definition of security to improve clarity.** Allowing opt-outs and installations or uninstallations of security software applications undermines the security of the entire cyber ecosystem and its users. The word "necessary" in this section could undermine the utility of the security exemption added in the Senate bill, as it is too limited. Moreover, the security exemption is only applicable to this provision, creating a confusing mix of legal requirements.
Affirmative Defenses 3(b)(1)(A-C) Preventing violations of, or complying with, federal or state law; protecting user safety, non-public data, platform security; and maintaining or enhancing the core functionality of the platform.	**Amend this provision to remove the need for an affirmative defense for security actions or to exclude security broadly by adding a separate security exemption section.** Affirmative defenses place the burden of proof on platforms to justify exclusionary actions that may be construed as harmful to competition. For example, it is unclear whether spam and fraud activity, while not impacting the core functionality of a platform but having significant impact on a platform's credibility and user safety, would serve as a justifiable exemption to limit competitor products. Determining what is and is not lawful could drastically slow the platform's process of implementing policies, safeguards or defenses against adversarial cyber activity.