SECURITY IN ANTITRUST: IMPLICATIONS OF TWO HOUSE BILLS

November 2021

Over the past several months, Congress has identified and prioritized the need to address what they see as unregulated behavior in large tech companies. By taking a look at two of the House bills which address antitrust regulation, this explainer analyzes sections which we believe will have detrimental, unintended, third-order effects on cybersecurity. Security at the pace of bureaucracy is anathema to the growth of a cybersecurity mindset and improved cybersecurity. Therefore, given the cybersecurity ramifications of these provisions, we recommend amending or removing existing language to address these concerns.

The analysis focuses squarely on the cybersecurity and data protection concerns of the identified provisions, and does not address the raging debate on the merits of the antitrust proposals more broadly, which R Street has come out against.

Rep. David Cicilline's (D-R.I.) American Choice and Innovation Online Act (HR3816)

Introduced in the House of Representatives on June 11, 2021, the American Choice and Innovation Online Act aims to ban discriminatory conduct by covered platforms.

SECTION	TEXT	DATA SECURITY IMPLICATIONS	RECOMMENDATION
Section 2(b) Unlawful Discriminatory Conduct (General Prohibitions)	Make it unlawful to restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware and software features that are available to the covered platform operator's own products, services or lines of business.	This provision would more than likely open up devices to more cybersecurity vulnerabilities. Apple argues, among others, that this will impact its ability to provide security assurances through its app store by no longer requiring apps to go through the App Store. Apps from any 3rd party, verified or not, would be allowed on iPhones, potentially through sideloading.	REMOVE
Section 2(b) Unlawful Discriminatory Conduct (General Prohibitions)	It shall be unlawful for a person operating a covered platform, in or affecting commerce, to engage in any conduct in connection with the operation of the covered platform to— • restrict or impede covered platform users from uninstalling software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator • restrict or impede business users from communicating information or providing hyperlinks on the covered platform to covered platform users to facilitate business transactions.	This could restrict platforms from excluding malicious apps, spammers, websites and hyperlinks. Pre-installed software can include security tools and safety measures, and covered entities should not be restricted from pre-installing security measures on their devices or programs, and allowing users to remove pre-installed security software would make their devices vulnerable to attack.	AMEND to: • allow the exclusion of malicious apps, spammers, websites, hyperlinks and any other security risks from the requirements for communication and transactions. >Such a provision should include an amendment providing additional clarity on the legal standard to determine exclusions • include a savings clause for pre-installed security software to exclude them from the requirement to allow pre-installed app deletion • clarify the term "business user" to ensure bad actors cannot use that cloak of legitimacy for malicious activity.

*Required as part of a report

	It shall be unlawful to: restrict or impede a business user from accessing data generated on the platform by the activities of the business user or its customers through an interaction with the business user's products or services, such as contractual or technical restrictions that prevent the portability of such data by the business user to other systems or applications.	Requiring, by law, all covered entities to interact with all third parties precludes those companies from excluding unsafe and unverified vendors from gaining access to data or opening up connections with unsafe third parties. Additionally, expanding the definition of data to include behavioral profiles and the non-direct information could also open more security risks as that data is shared and more entities have access to that data.	AMEND to include a risk assessment or security liability exclusion for interoperability or data sharing with third parties.
Section 2(b) Unlawful Discriminatory Conduct (General Prohibitions)	The term ''data'' shall include information that is collected by or provided to a covered platform or competing business or a potential competing business that is linked, or reasonably linkable, to a specific user or customer of the covered platform or a competing business or a potential competing business.	The bill should clarify that inference or behavioral profiles are not part of data that can be shared between companies. A savings clause could help protect this data from being shared and unauthorized access.	AMEND to clarify the term "data." Most importantly, this bill should anticipate a national data security and privacy bill, and prepare to be interoperable with such a law.
	A covered platform may not: "Use non-public data obtained from or generated on the platform by the activities of a business user or its customers that is generated through an interaction with the business user's products or services to offer or support the offering of the covered platform operator's own products or services."	The restriction on internal platform data sharing (which could be read to include data sharing across products) is problematic from a security perspective as it could prohibit sharing across products for the purposes of flagging malicious activity through identifying patterns of behavior. • Focus on non-public data may incentivize the publication of larger amounts of user data in order to use it to create competing products and services, weakening data privacy.	AMEND to: • affirmatively allow the sharing of data across platforms and products to enable pattern tracing and tracking of malicious activity. • clarify the rules around publication of data solely for the purpose of using it to create competing products or services.

Rep. Mary Gay Scanlon's (D-Pa.) Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021 (HR3849)

Introduced in the House of Representatives on June 11, 2021, the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021 aims to promote competition, lower entry barriers, and reduce switching costs for consumers and businesses online.

SECTION	TEXT	DATA SECURITY IMPLICATIONS	RECOMMENDATION
Section 4(e)	"A covered platform may not make a change affecting its interoperability interfaces without receiving approval from the Commission if that change is necessary to address a security vulnerability or other exigent circumstance that creates an imminent risk to user privacy or security if the change is narrowly tailored to the vulnerability and does not have the purpose or effect of unreasonably denying access or undermining interoperability for competing businesses or potential competing businesses."	This language is completely anathema to the structure that has been adopted and advocated by security experts. Changes are made weekly, if not daily, for the purposes of security, and conditioning those updates on Federal Trade Commission (FTC) approval would slow down and therefore weaken security throughout U.S. networks. The definition of "exigent" and "imminent" may very well only cover a small portion of security vulnerabilities.	REMOVE for the purposes of cybersecurity and effective patching and updating.
Section 4(b)(1)	"A competing business or a potential competing business that accesses an interoperability interface of a covered platform shall reasonably secure any user data it acquires, processes, or transmits, and shall take reasonable steps to avoid introducing security risks to user data or the covered platform's information systems."	Putting all data security responsibility on the "accessing" organization incentivizes the wrong type of security behavior from organizations handling data. It may also limit covered entities' ability to determine whether an accessing organization is a malicious user.	AMEND to incentivize strong data security practices across covered entities and accessing organizations. Rules about reasonable steps on securing user data should apply equally to all data holders.

Section 4(e)(1)	Directs the FTC to create standards for portability and interoperability that "protect data security and privacy" through technical committees designed by the FTC. The committees "meet regularly to provide information, analysis, and recommendations to the Commission on the standards of portability and interoperability and any changes to those standards" including "data security and privacy protections for data portability and interoperability."	Conditioning security patching and updates on FTC approvals is basically security at the pace of bureaucracy, and would be detrimental to the security of U.S. networks. The status of pending data security and data privacy (DSDP) legislation is also unclear. A secondary law addressing some, but not all, data security and data privacy issues could create a patchwork regulatory framework which would complicate the existing complex web of DSDP regulation at the state level.	National data security and privacy legislation should precede any other laws surrounding broader data security and privacy mandates.

These two bills, among the other antitrust bills that have been introduced, have three of the same challenges. They try to address antitrust concerns, but by doing so, they undermine the security of the networks the covered platforms control. First, they require more data to be shared and interoperable, opening up new and undetermined avenues for security threats and data leaks through unverified third parties. Second, as they require interoperability with third parties, they restrict or reduce the ability of entities themselves to use data available across their own platforms to create cheaper, more effective solutions for their customers. Third, these provisions include unacceptable obstacles to security improvements through conditioning updates and patches on FTC approval prior to implementation. Lastly, provisions in these bills impinge on the work of data security and privacy experts who are making strides to improve security through comprehensive legislation, and may be counterproductive to overarching data security goals. Unfortunately, Sen. Amy Klobuchar (D-Minn.)'s American Innovation and Choice Online Act (S. 2992) takes a similar guilty-until-innocent approach, which mentions security in only one of seven prohibited practices and would have much the same chilling effect on security as the House bills.

Saying nothing of the debates on the merits of the antitrust arguments, these bills create significant challenges to improving the cybersecurity and data security and privacy of users and networks. At a minimum, these provisions should be amended or removed as the House debates these bills.

CONTACT US

For more information on the subject, contact
Tatyana Bolton
Policy Director, Cybersecurity and Emerging Threats
tbolton@rstreet.org