Our last explainer focused on the American Choice and Innovation Online Act (H.R.3816) and Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021 (H.R.3849). This explainer analyzes S.2992, the American Innovation and Choice Online Act, the Senate version of H.R.3816. Like the House versions of antitrust legislation, this bill includes provisions which have significant negative cybersecurity ramifications.

This analysis is based on the manager's amendment to the bill from Jan. 18, 2022. It 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.

American Innovation and Choice Online Act (SB 2992)

Section	Text	Data Security Implications	Recommendation
Unlawful Conduct Section 3(a)(4)	It shall be unlawful for a person operating a covered platform, in or affecting commerce, if it is shown, by a preponderance of the evidence [greater than 50%], that the person has engaged in conduct that would: materially restrict, impede, or unreasonably delay the capacity of a business user to access or interoperate with the same platform, operating system, or hardware or software features that are available to the products, services, or lines of business of the covered platform operator that compete or would compete with products or services offered by business users on the covered platform; …	This provision would more than likely open up devices to more cybersecurity vulnerabilities. Apple argues 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 third party, verified or not, would be allowed on iPhones, potentially through sideloading.	REMOVE
Unlawful Conduct Section 3(a)(7)	It shall be unlawful for a person operating a covered platform, in or affecting commerce, if it is shown, by a preponderance of the evidence, that the person has engaged in conduct that would: … materially restrict or impede a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the products or services of the	Broader privacy provisions and consumer rights are implicated by this, but not in a comprehensive way. Without comprehensive legislation, the approach would be piecemeal and have minimal effect on privacy, or none at all. This provision would expand business user access and could jeopardize data security if the business user is an unverified third party that does not	REMOVE

	business user, such as by establishing contractual or technical restrictions that prevent the portability by the business user to other systems or applications of the data of the business user; …	employ adequate safeguards.	
Unlawful Conduct Section 3(a)(8)	It shall be unlawful for a person operating a covered platform, in or affecting commerce, if it is shown, by a preponderance of the evidence, that the person has engaged in conduct that would: … unless necessary for the security or functioning of the covered platform, materially 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; …	As discussed in our previous explainer, it is critical that security moves at the most expeditious pace possible. 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 that was added in the Senate bill as it is too limited. Moreover, this section lists unlawful conduct, but the security exemption is only applicable to one provision, creating a confusing mix of legal requirements.	AMEND section to exclude security applications or processes from the restrictions for user freedom-of-choice on platforms. AMEND provisions (4) - (10) related to unlawful conduct to include security exemptions or make a stand-alone security provision applicable to (4) - (10). AMEND definition of security; the term should be clearly defined.
Affirmative Defenses 3(b)(2)(B)(i)	It shall be an affirmative defense to an action under paragraph (4), (5), (6), (7), (8), (9), or (10) of subsection (a) if the defendant establishes by a preponderance of the evidence that the conduct - (B) was narrowly tailored, could not be achieved through less discriminatory means, was nonpretexual, and was reasonably necessary to - *(i) prevent a violation of, or comply*	The word 'necessary,' as applicable to the affirmative defense for preventing a violation of law, is too narrow here. Not all security incidents break the law, since security-conscious companies act on early warning signals—like login attempts from other countries—to handle spam or malicious acts. These are not violations of law, but companies should still be encouraged to take action	AMEND to remove the requirement for affirmative defense for security actions -OR- AMEND to exclude security in a broader way by ADDING a security exemption before the affirmative defense section, or at the end of the bill.

	with, Federal or State law;	when facing early indications of a threat or malicious takeover of users accounts. This could also restrict cross-platform broad security updates because of the requirement for narrow tailoring of updates.	
Affirmative Defenses 3(b)(2)(B)(ii)	It shall be an affirmative defense to an action under paragraph (4), (5), (6), (7), (8), (9), or (10) of subsection (a) if the defendant establishes by a preponderance of the evidence that the conduct - (B) was narrowly tailored, could not be achieved through less discriminatory means, was nonpretexual, and was reasonably necessary to - *(ii) protect safety, user privacy, the security of non-public data, or the security of the covered platform;*	Definition in this subsection is likewise too limited and does not include public data. Most unfortunately, because these provisions have strict restrictions and few, confusing security exemptions, as well as a requirement for an affirmative defense for actions, the incentive for development and implementation of security policies, patches and product improvements would be weakened. With stringent requirements saved by only a few security exemptions, the section also requires an affirmative defense. This section subsequently threatens incentives for effective security policies and product improvements by slowing down on what need to be quick patching processes.	REMOVE
Affirmative Defenses 3(b)(2)(B)(iii)	It shall be an affirmative defense to an action under paragraph (4), (5), (6), (7), (8), (9), or (10) of subsection (a) if the defendant establishes by a preponderance of the evidence that the conduct - (B) was narrowly tailored, could	"Core functionality of the platform" is vague, and may preclude covered entities' taking actions such as blocking spam and excluding malicious apps from an app store. This is opposed to the core tenets of	REMOVE

	not be achieved through less discriminatory means, was nonpretexual, and was reasonably necessary to - *(iii) maintain or substantially enhance the core functionality of the covered platform.*	cybersecurity and will inevitably introduce, at a minimum, another layer of review or consideration which would slow the process of implementing policies, safeguards, or blocking adversary activity. In many cases, security actions may need to be precisely NON-narrowly tailored to address security threats.	

Bill authors note, "As dominant digital platforms … increasingly give preference to their own products and services, we must put policies in place to ensure small businesses and entrepreneurs still have the opportunity to succeed in the digital marketplace." Assuming the bill would actually promote this, the cost would be high: broad cybersecurity and data protection weaknesses. The manager's amendment to this bill acknowledges some cybersecurity concerns, but fails to address the main concerns outlined here. On the whole, it is difficult for security experts to encourage resilience and diligence for platforms and networks along with the uptake of strong cybersecurity practices. It is even harder to convince businesses that cyber risk is a business risk, or encourage them to develop products with security in mind. While this is not a strict cybersecurity bill, it adds obstacles and restrains the application of security safeguards by platforms, which creates adverse incentives.

This bill would punish companies with a business model that focuses on security. From a policy perspective, we should encourage—not discourage—more companies to include more stringent security for all products, especially software that is sold at scale to millions of users. Forced interoperability, narrow requirements and obstacles for security updates through requirements for affirmative defense, as well as patchy security exclusions, create a recipe for weaker cybersecurity and should be reconsidered, amended or removed before any further movement on this legislation.

In terms of data security and protection, any provisions should be considered separately in a comprehensive bill, not as a portion of an antitrust bill. This is a challenging area with many tradeoffs that need to be carefully considered to achieve a suitable balance between consumer protection and business function, and an anti-trust bill is not the place to debate or determine these tradeoffs.

For more information on the subject, contact:

Tatyana Bolton
Policy Director, Cybersecurity and Emerging Threats
tbolton@rstreet.org