DON'T BREAK WHAT WORKS

AICOA MANAGER'S AMENDMENT DOES NOT ADDRESS THE BILL'S UNDERLYING PRIVACY, CYBER, AND NATIONAL SECURITY CONCERNS

As the American Innovation and Choice Online Act (S.2992) moved through committee in January, Senators expressed concerns over the bill's national and cyber security flaws—which could cede ground to technology rivals in China, Russia, and other countries, require data sharing with foreign competitors, harm consumer privacy, and limit actions that American companies can take to address bad actors.

To purportedly address these concerns, the bill's sponsors offered a manager's amendment. While the amendment acknowledges key weaknesses in the bill, it does not adequately address them. In fact, in some places, the amendment makes S.2992 even more harmful to American companies and national security.

The Concerns Below Were Raised At The January Markup And Still Have Not Been Addressed By The Sponsors:

S.2992 would threaten Americans' privacy

Flaws:

Sen. Patrick Leahy (D-VT)

"The bill makes it too difficult for online platforms to adequately protect consumers' privacy. The bill creates a bar far too high for platforms to protect privacy without worrying about being penalized."

Sen. Jon Ossoff (D-GA)

"Striking the appropriate balance between privacy and cybersecurity in this legislation is important. And what I want to offer is a second-degree amendment, Senator Lee, to yours that we toughen the standard slightly that these tech companies have to meet in order to invoke this affirmative defense where privacy or security functionality is concerned."

Does the manager's amendment address any of these concerns?

No. The manager's amendment expands the term "business user" to include corporations and associations that use or are "likely to use a covered platform for the advertising, sale, or provision of products or services." As in the underlying bill, the definition of "data" is not specific. It "includes information that is collected by or provided to a covered platform or business user that is linked, or reasonably linkable" to a specific user or customer on the covered

platform or simply a user or customer of a business user. It is unclear what "linked" or "linkable data" is in the first instance. This addition would limit the covered platform's ability to maintain user privacy, data security, and to engage in meaningful content moderation.

See more here.

S.2992 would make Americans more vulnerable to cyber attacks

Flaws:

Sen. John Cornyn (R-TX)

"I think we've all learned that unvetted access to data, hardware, and services raises cybersecurity concerns. Not every potential user that does want to interoperate with a platform will have the level of cybersecurity that Americans deserve. The Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency at the Department of Homeland Security have issued a joint threat alert warning that Chinese state-sponsored cyber actors target the United States repeatedly —I think that's common knowledge. This bill would make those targets more vulnerable."

Sen. Dianne Feinstein (D-CA)

"This bill would actually prevent companies [like Apple] from taking steps to ensure that an application is safe before you download it from your phone. We're requiring companies to take down protections that are in place today and instead allowing hackers, and those looking to steal, to access devices."

Does the manager's amendment address any of these concerns?

No. The amendment introduces a "rule of construction" which states that covered platforms can refuse to interoperate or share data with entities that are on sanctions lists or present national security threats. But not all dangerous actors are on sanctions lists, especially foreign adversary-designed apps seeking to collect data on Americans, fraudsters, and counterfeiters. The amendment thus indicates that covered platforms could not cut off suspected or even known bad actors unless those bad actors have been sanctioned by the U.S. national security apparatus.

See more here.

S.2992 would harm American national security

Flaws:

Sen. John Cornyn (R-TX)

"Mr. Chairman, I'm concerned about the potential national security consequences of this bill. I'm worried that it will harm American business and reward our adversaries, most notably the People's Republic of China. The last thing that we should be doing is weakening America's ability to compete in a global economy. I worry that this bill, by disadvantaging American companies, will basically be a big gift to the People's Republic of China. It serves our homegrown companies up on a platter and does nothing to impact the bad conduct of our adversaries."

Senator Chris Coons (D-DE)

"I have significant concerns to balance about whether this bill achieves the right balance between the costs and inefficiencies between litigation and compliance and potentially unintended consequences on the competitiveness globally of our digital democracy principles on the world stage and whether or not we are achieving enough progress on combating anti-competitive behavior on the other."

Senator Tom Cotton (R-AR)

"I have concerns with provisions in the bill that could require data sharing between American companies and bad actors under the control of the Chinese Communist Party. I don't think that's the intent of the bill or the drafters based on our conversation but I do think we can improve that language to make it safer for our companies and citizens."

Does the manager's amendment address any of these concerns?

No. The manager's amendment changes revenue thresholds such that it applies to private companies with $30B in revenues and 50M U.S. users, publicly traded companies with revenues of $550B, and to companies with at least 1B worldwide users. The amendment does little to extend commitments to many foreign tech rivals like Huawei, Baidu, Yandex, because few such firms currently meet the 50M U.S. user threshold or the 1B worldwide user threshold. The amendment thus bypasses current realities and will sweep in other firms, including large private U.S. accounting, financial services, and insurance firms, as well as retailers which meet those thresholds. This would dramatically hamstring the U.S. economy, knee-capping U.S. digital services while giving a pass to foreign rivals and missing its likely target: Chinese digital leaders.

To date, even after the January 2022 markup, the bill sponsors have failed to address these Senators' concerns or incorporate feedback into the final bill before it goes to the floor.

See more here.