DON'T BREAK WHAT WORKS

THIRD TIME'S THE CHARM? SENATOR KLOBUCHAR'S AICOA 3.0 ACKNOWLEDGES ALL OF THE BILL'S PROBLEMS; FIXES NONE

During the Senate Judiciary Committee markup of Senator Klobuchar's antitrust bill, **14 senators** expressed serious reservations and said they would not vote for the bill on the Senate floor as drafted. After months of promising that there would be an open process that would address national security, privacy, content moderation, and other concerns, Senators Klobuchar and Grassley released an updated version of the American Innovation and Choice Online Act, with little input from colleagues or experts in the field. So what has changed? Almost nothing - and in some areas, it's gotten worse.

National security leaders have **repeatedly warned** that the bill would require sharing of data and infrastructure with foreign competitors while leaving companies like Alibaba and Tencent unscathed. The new draft includes:

- **The same disadvatages for American firms:** Still discriminates against American companies in favor of Chinese, Russian, and other foreign competitors, and allows these foreign rivals to access American data and infrastructure.
- **No changes to impacts on cybersecurity tools:** U.S. companies will face lawsuits for removing foreign cyber threats and deploying best-in-class cybersecurity tools, including systems that detect and block spam and malicious emails, and 'safe browsing' services that block malicious threats on over four billion devices every day.
- **A disregard for emerging security threats:** Many AICOA provisions create national security risks, but there is new security language in **just one** of the bill's ten provisions, **and** it only applies when access would "lead to a significant cybersecurity risk," leaving companies open to litigation for every cybersecurity decision if the FTC or a court thinks there was just a "moderate" or "emerging" cybersecurity risk. **This standard is simply unworkable:**
    - Companies often don't know which emergent security threats are "significant" and which are moderate or minor when taking preventive action to ward off a potential attack. This standard requires them to guess on the front end with drastic consequences for getting it wrong.
    - This language also misunderstands the modern security threat landscape, which increasingly involves smaller and decentralized foreign actors that can swarm together at unpredictable moments. If US companies are forced to give these actors access to data and infrastructure until they cross an arbitrary threshold of being a "clear" and "significant" threat, then it will already be too late.

Privacy experts have expressed major concern that the bill would jeopardize the safety and privacy of American consumers by restricting companies' ability to apply security standards and forcing data-sharing with third parties, including foreign firms. However, the revised version:

- **Still prohibits the removal of bad actors:** Section 2(a)(2) is still intact and still prevents the removal of bad actors, which would flood devices with associated privacy and security risks
- **Keeps vague definitions of data:** It remains unclear what data can be classified as "linked" or "linkable" to a business user
- **Still contains unreasonable penalties:** The bill requires companies to give up to 10% of their U.S. revenue for the period in which the bill violation occured. Coupled with the vague provisions of the bill, this disincentivizes companies from aiming to protect privacy in a way that might violate the bill's language.

Content moderation concerns remain and are in fact worsened because this bill:

- **Still does nothing to protect responsible efforts by covered platforms to moderate hateful speech, disinformation, or other abusive content.** No changes have been made to Section 3(b) that would protect a covered platform's ability to make decisions to protect user access to authoritative and high-quality information.
- **Doubles down on limiting content moderation** by making clear that it is unlawful to act "in a manner that is inconsistent with the neutral, fair, and non-discriminatory treatment of all business users" in Sec. 3(a)(9). Under the original language, it was an open question as to whether covered platforms could perhaps establish their own standards.
- **Puts the burden on a covered platform to defend content moderation decisions** by adding new language stating explicitly that the defendant "has the burden" of proving an affirmative defense.
- **Politico**: A spokesperson for California Democratic Sen. Alex Padilla said the senator still has concerns about a provision that he believes could undermine efforts to combat hate speech and disinformation.

Special interests like big telecom and payment company lobbyists have gotten carveouts in the new version of the bill..

- The revised verison protects big banks, telcos, and credit card companies. The bill addresses corporate lobbyists' concerns with new language that explicitly protects big telcos like AT&T and big payment companies like Visa by changing the definition of what is an "online platform" regulated by the bill.

Meanwhile, language in the legislation still exacerbates record-high inflation. **Studies** have shown that digital services can combat inflation.

Finally, the new version **doesn't even attempt to address the many concerns around breaking free products that consumers enjoy, empowering small businesses, and providing important social benefits** like emergency and natural disaster preparation, connection with family and friends, and access to free, educational information.