

# Bills Targeting Successful American Companies Undercut Data Security and Privacy Goals

Lawmakers on both sides of the aisle have offered support for smart, strategic privacy and data security measures. Often, the difficulty in achieving those goals lies in the details. Some members of Congress have pushed to pass bills, including the American Innovation and Choice Online Act (AICOA) and Open App Markets Act (OAMA), that would undermine Americans' privacy and undercut data security protections.

## Here's how bills targeting top American companies would undermine bipartisan privacy and data security goals:

Instead of protecting sensitive information online, bills like AICOA and OAMA would weaken privacy and data security protections.

- **AICOA threatens to expose Americans' private data to bad actors.**
  - Top U.S. companies provide Americans with privacy while using popular products and services. However, AICOA treats privacy as an afterthought. The bill [includes](#) sweeping interoperability requirements and would force companies to provide third parties with broad access to Americans' data.
- **AICOA includes provisions that would weaken cybersecurity.**
  - American businesses take robust security measures to protect users online from foreign and domestic bad actors by protecting individuals' data and blocking malware and viruses. AICOA would [undermine](#) key cybersecurity protections that keep products that millions of Americans enjoy using, like the cloud or popular smartphones, safe.
- **OAMA would get rid of security measures that consumers, businesses, and governments rely on.**

- App stores currently have the ability to vet apps for security concerns and remove apps that present a risk to users. These security controls can [provide](#) a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps without impacting system integrity. OAMA would remove the vetting process that ensures apps on an app market meet rigorous safety standards.
- **The current app store model includes tools that are critical for online privacy. OAMA would force companies to remove those tools.**
  - Currently, app stores have the ability to put in place limits on how much user data can be collected and used for tracking by third-party apps. However, proposed legislation, like OAMA, would [mandate](#) the removal of the same privacy and security tools American companies have put in place to ensure that vulnerable third-party apps are not offered to users.

## What the experts are saying:

Top industry experts agree that bills like AICOA and OAMA would undermine efforts to strengthen privacy and data security protections.

- **[Danel Savickas, Taxpayers Protection Alliance](#)**
  - “Lawmakers in Congress — and in state houses across the nation — should not be punishing successful American companies for providing useful products and services while keeping their infrastructure secure. App stores have created an ecosystem that connects startups, developers, and entrepreneurs to their respective audiences through increased market access. This gives these groups significant advantages that would not otherwise be possible. Additionally, the stores provide customers with trust through the privacy and security precautions built in by design.”
- **[Brandon Pugh, R Street Institute](#)**
  - "The direct call for “serious federal protections for Americans’ privacy” was a good step, although combining it with a slew of anti-Big-Tech rhetoric and broader controversial tech measures reduced the effectiveness of this call and overshadowed the privacy focus...Data privacy and security risks do not depend on company size. There are countless examples of small and medium-sized companies, and even large non-tech companies, employing terrible data privacy and security practices involving highly sensitive data. Relatedly, we should keep action on privacy focused on privacy. Adding in other controversial measures,

like antitrust, content moderation and Section 230, are sure ways to stall progress."

- [Anna Bosch, The App Association](#)

- "(Cybersecurity and Infrastructure Security Agency) Director Easterly's comments highlight that tech legislation should incent and encourage businesses to take measures that protect consumers, rather than punish them for doing so. Proposals like AICOA and OAMA would weaken cybersecurity and consumer privacy, putting a disproportionate burden on consumers to protect themselves and introducing new, unjustified risks of decreasing trust in the tech ecosystem."

- [Shane Tews, American Enterprise Institute](#)

- "However, legislation like the Senate's AICOA and OAMA, along with the DMA, would do the opposite of what has been recommended by cybersecurity experts. These bills want to mandate that current app store review practices — such as privacy tools and processes put in place to mitigate security risks like malware applications or dark web cyber tools — be dismantled in the name of competition...There are plenty of hostile and malicious actors in the world today searching constantly for new ways to access consumers' devices, data, and homes. And it seems a particularly bad time to make our critical digital infrastructure more vulnerable by deterring our most important platforms from protecting their own systems and users. Platform decision-makers should not be given a choice of either letting suspicious third-party apps and entities into their ecosystems or facing the threats of complaints, investigations, litigations, injunction, and penalties."

## Unlike AICOA, there is broader bipartisan interest in strengthening data privacy and security protections:

- In the Senate, Republicans like Senator Roger Wicker have underscored the need for a federal privacy standard. Senator Wicker is on the record [stating](#) that "with the recent increase in cyberattacks on our nation's critical infrastructure...the need for federal privacy legislation is imperative." Similarly, Democratic lawmakers, including Senator Ed Markey have [pushed](#) for Congress' upper chamber to act.

- In the House of Representatives, powerful committee chairs, like Congresswoman Cathy McMorris Rodgers and Congressman Frank Pallone have [endorsed](#) the idea of working to “establish national data privacy protections for all Americans.”

**Major American tech companies support the passage of a federal consumer privacy law.**

- [Amazon](#) and [Google](#), for example, have both publicly encouraged leaders in Washington to pass a comprehensive federal privacy law, and both have committed to working with lawmakers to protect Americans’ sensitive data and privacy.
- Similarly, trade organizations that represent major American tech companies have issued statements of support for policy solutions that would ensure Americans have a baseline of federal consumer privacy protections. [CCIA](#), for example, has endorsed a federal privacy framework that would “set consistent transparency requirements, consumer controls, and accountability measures for data controllers, while empowering the Federal Trade Commission to carry out robust enforcement.”