DON'T BREAK WHAT WORKS

dontbreakwhatworks.ccianet.org

OAMA Threatens Cybersecurity, Privacy, and Competition

At a time when Americans have made it clear that they are most concerned about stopping scams and malware, the reintroduced Open App Markets Act (OAMA) would unfortunately limit efforts to combat these practices. OAMA has been widely criticized because it would undercut bipartisan privacy and cybersecurity goals, while also hindering competition and limiting consumers' options in app stores.

OAMA weakens privacy and cybersecurity protections, while limiting app store options that American consumers value.

- **OAMA undermines security measures that consumers and businesses rely on to keep Americans' data safe.**
  - App stores utilize robust security ecosystems to prevent fraudulent apps, data-harvesting schemes, and foreign surveillance tools. Yet, OAMA would force companies to abandon thorough app review and vetting processes, undermining prompt responses to infringing content or apps that fail to meet minimal security requirements. As a result, malicious actors—including state-sponsored actors from adversarial nations—would gain additional access points to American devices and data.

- **OAMA limits competition and hurts app developers and consumers.**
  - The market for app development is flourishing. Innovation attracts consumers, which further reinforces development and competition. Much like app stores that enforce strong security features, developers are also incentivized to build strong safety features into their apps to gain consumer trust. Unfortunately, OAMA includes provisions that outlaw features that consumers love and rely on, which would discourage developers from creating quality, innovative apps.

- **OAMA would force all platforms to operate under inconsistent rules.**
  - Rather than allowing security and engineering experts to develop a safe balance between security and interoperability, a federal mandate which courts will interpret in conflicting ways will become the new standard of compliance. Consumer safety demands should drive key security decisions, not policymakers or courts who may lack necessary expertise and technical knowledge.

Experts agree that OAMA would limit competition, hurt consumers, and undermine efforts to strengthen privacy and cybersecurity protections:

- **David Williams, Taxpayers Protection Alliance**
  - "OAMA erodes critical cybersecurity protections and parental controls on smartphones, putting tech companies in the role that ought to be reserved for parents and caretakers . . . Supporters of OAMA falsely claim that the bill will expand consumer choice. Paradoxically, the bill would, in fact, reduce consumer choice. Consumers have consistently shown a demand for simpler and closed smartphone ecosystems that prevent users from invertedly downloading malicious software."

- **Morgan Reed ACT | The App Association**
  - "Without a federal privacy and data security framework, this bill sacrifices consumer protections and small businesses to fill the coffers of multi-billion-dollar companies that want free distribution from mobile platform operators. This is another example of how small businesses and entrepreneurs are being crushed underfoot while 800-pound gorilla tech companies are fighting it out."

- **Brian McMillan, Computer & Communications Industry Association**
  - "Bad actors pose an enduring threat to the users of digital goods and services, so businesses need flexibility to perform security, trust, and safety operations. OAMA would interfere with these efforts by limiting digital ecosystems' ability to respond to content or ban apps that don't meet their privacy or safety requirements."

- **Software Information Industry Association**
  - "OAMA threatens to gut the security features built into today's app stores, all while reducing consumer choice and handing sensitive data to bad actors. This bill doesn't open markets, it breaks them along with all the digital tools Americans rely on."

- **Patrick Hedger, NetChoice**
  - "OAMA forces American companies to permit sideloading of potentially hazardous apps and strips app stores of their ability to vet bad actors, effectively opening up secure U.S. tech systems to our geopolitical rivals on a silver platter. That's not competition — it's sabotage that will harm families first to benefit rival, foreign software companies."