ACT
The App Association

How the American Innovation and Choice Online Act (S. 2992) Would Undermine App Stores

S. 2992 seeks to undo the current management structures of large, privately managed marketplaces, including software platforms (app store / operating system combinations). The provisions seek to limit actions large platforms take that would advantage their own offerings or disadvantage other offerings. The central provisions of S. 2992 require open access to personal information and operating system and device features. As a result, S. 2992 requires software platform operators to allow sideloaded software and app stores by default. Some of the largest sellers on the app stores support S. 2992 because it would force software platforms to distribute their products for free. However, S. 2992 would ultimately do a lot more harm than good.

More Malware, Copycat Apps, and Fraudulent Reviews.

Software platforms would no longer be able to reject or remove bad actors, trojan horse apps, malware, etc., from consumer devices.

a. Worse or Nonexistent Services. The bill would outright prohibit many of the services our member companies have pushed the platforms to perform better—from removing copycat apps and malware to eliminating apps with fake / fraudulent reviews. App makers would be on their own.

Fewer Choices for Developers.

Right now, app makers have a choice between HTML, progressive web apps, Android, iOS, etc., and mobile app stores are often the best option because they are closed ecosystems. The bill would mandate that mobile software platforms operate like the other available options, homogenizing what is currently a diverse market for distribution.

Increased Cyberattacks on Mobile Devices.

Without needing to bypass platform level security features to reach users, cybercriminals could target smart devices with much greater precision and volume (currently, a only small fraction of Android devices are "soft" targets because they allow sideloading from specified sources)—which means a lot more text and other behavioral attacks on mobile consumers.

Higher costs for smaller companies.

By requiring software platforms to provide free distribution for the highest-grossing, digital-only goods and services, the bill would upend the current " progressive" structure—charging the highest-revenue sellers more in commissions— and push software platforms to a more "regressive" structure, charging low-revenue and the 84 percent of app makers that sell real-life goods and services more.

a. Disintegrated Trust Infrastructure. Another cost would materialize in the form of trust-building: on app stores, vetting apps and app makers for security and privacy would be consumers' job rather than software platforms', resulting in consumers turning away from small companies without brand recognition.

SEC 3. UNLAWFUL CONDUCT

(a) In General,— It shall be unlawful for a person operating a covered platform in or affecting commerce to engage in conduct, as demonstrated by a preponderance of the evidence, that would—

How The American Innovation and Choice Online Act (S. 2992) Undermines Important App Store Management Functions

(4) 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;

Platform Access. This provision would prohibit a software platform from removing bad actors from the app store. There is no exception here for apps that steal data or even for apps that spread malware.

(7) 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 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;

Personal Data. This provision would prohibit an app store from restricting any app's access to personal data, even if the app presents serious privacy and security threats

(b) AFFIRMATIVE DEFENSE—

(1) IN GENERAL,—it shall be an affirmative defense to an action under paragraph (1), (2), or (3) of subsection (a) if the defendant etablishes by a preponderance of the evidence that the conduct was norrowly tailored, nonpretextual, and reasonably necessary to—

(B) protect safety, user privacy, the security of nonpublic data, or the security of the covered platforms;

Security is Illegal. The only way for a platform to rebut the presumption that removing or rejecting malware or other bad actors is legal is to show that doing so was **"narrowly tailored, nonpretextual, and reasonably necessary to"** protect security or privacy. A platform would not know if a privacy or security practice were legal unless it were sued and offered an affirmative defense based on the privacy or security practice.

ACT | The App Association

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org/ actonline.org