ACT
The App Association

How the Open App Markets Act (S. 2710) Would Undermine App Stores

S. 2710 seeks to undo the current management structure for mobile app stores. The provisions track some of the complaints from the largest companies selling digital-only goods and services on the app stores, which have an ultimate purpose of forcing app stores to distribute their products for free. As a result, S. 2710's centerpiece is a mandate for software platform operators to allow sideloaded software and app stores by default. In addition to the sideloading mandate, S. 2710 would also require software platforms to provide open access to hardware and software features for app makers, equal to the platform offerings' own access. These provisions could help some app companies obtain free distribution of their products in the short run, but that distribution service would be mandatorily devalued and 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.

How The Open App Markets Act (S. 2710) Undermines Important App Store Management Functions

> (d) Interoperability. — A covered company that controls the operating system or operating system configuration on which its app store operates shall allow and provide readily accessible means for users of that operating system to—
>
> (1) choose third-party apps or app stores as defaults for categories appropriate to the app or app store;
> (2) install third-party apps or app stores through means other that its app store, and
> (3) hide or delete apps or app stores provided or preinstalled by the app store owner or any of its business partners.

Sideloading mandate. This provision would force mobile platform operators to allow unvetted, sideloaded software—including malware, spyware, and other apps that only exist to harm consumers—onto consumer devices by default.

> (f) OPEN APP DEVELOPMENT.— A covered company shall provide access to operating system interfaces, development information, and hardware and software features to developers on a timely basis and on terms that are equivalent or functionally equivalent to the terms for access by similar apps or functions provided by the covered conmpany or to its business partners.

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.

> (b) REQUIREMENTS.—Subsection (a) shall only apply if the covered company establishes by a preponderance of the evidence that the action described in that subsection is—
>
> (1) applied on a demonstrably consistent basis to—
>
> (A) apps of the covered company or its business partners;and
> (B) other apps;
>
> (2) not used as a pretext to exclude, or impose unneccessary or discriminatory terms on, third party apps, in-app payment systems, or app stores; and
>
> (3) narrowly tailored and could not be achieved through a less discriminatory and technically possible means.

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 **"applied on a demonstrably consistent basis . . . not used as a pretext to exclude . . . and could not be achieved through a less discriminatory … means."** This is an extraordinary burden to put on a privacy or security measure to protect consumers.