ICLE tl;dr

The Open App Markets Act

February 2022

tl;dr

Background: The U.S. Senate is considering legislation—S. 2710, the Open App Markets Act—that would, among other restrictions, bar app stores from requiring app developers to use the store's own in-app payment system. The bill was introduced by Sen. Richard Blumenthal (D-Conn.), who has argued that it would "open the app economy to new competitors and give mobile users more control over their own devices."

But... The app store market is competitive and mobile users already have a choice of relatively open and relatively closed platforms. More open platforms, like the Google Play store, offer users the benefits of greater customization and a broader range of apps and payment options. More closed platforms, such as Apple's App Store, foreclose some of these options, but instead promise users greater privacy and security and a more curated experience that can ensure better device operation.

However... Requiring closed platforms to allow the use of alternative payment options would see large developers and rival payment processors get the benefit of the app store's investments without paying for them. The Open App Markets Act would substitute regulatory fiat for consumer choice, sacrificing the benefits currently enjoyed by many consumers.

KEY TAKEAWAYS

REMAKING THE APP STORE ECOSYSTEM

Under terms of the legislation, an app store with more than 50 million U.S. users could not require the use of an in-app payment system owned by that company as a prerequisite to access or distribute app software. Covered app stores also could not require apps to offer pricing or conditions at least as favorable as that offered through rival app stores.

The bill also would prohibit "unreasonable" self-preferencing by the app store in favoring its own apps over those of rivals, and would bar app stores from using nonpublic data gleaned from a third-party app to compete with that app. App stores would also be barred from "interfering" in communications between app developers and users.

Terms of the legislation would be enforced by the Federal Trade Commission and the U.S. Department of Justice, as well as state attorneys general. App developers also could exercise private rights of action against app stores for alleged violations of the law.

THE BENEFITS OF CLOSED APP STORES

So-called "closed" distribution models can improve user experience through curation, thereby excluding data-security threats and apps that might slow devices or crash frequently.

Like other platforms, app stores also have good reason to engage in self-preferencing, which will usually provide benefits to consumers by offering them cheaper, better, or more innovative product options.

App stores are multi-sided markets, and app developers benefit from access to the millions of users who access them. Any app store must balance the interests of both users and developers, as well as its own interests. Forcing a closed app store to allow the use of alternative payment methods could enable massive free-riding, thus undermining the incentives to develop such platforms in the first place, as well as the funding stream that allows platforms to invest in continuous development.

SECURITY RISKS OF SIDELOADING

The legislation also threatens to undermine user privacy and data security, both by directly removing app stores' ability to curate apps and by reducing their financial incentives and resources to invest in better cybersecurity tools. The result could be an app-store ecosystem in which hackers could operate, either for personal pecuniary gain or as part of coordinated terroristic or national security threats.

The legislation would mandate that app stores permit "sideloading": that is, installation of software on a mobile device outside of the approved app-store process. The sideloading mandate effectively prohibits an entire privacy and security-protection model, known as the "walled garden." By taking away the choice of a walled-garden environment, a sideloading mandate will effectively force users to use whatever alternative app stores are preferred by the developers of the applications that users wish to use.

Biden administration representatives to the Transatlantic Trade and Technology Council have acknowledged the potential cybersecurity threats of mandated sideloading in the context of similar mandates included in the European Union's proposed Digital Markets Act.

LACK OF TRANSPARENT ENFORCEMENT

The bill's text leaves unclear many important details about how it would be implemented, including exemptions for important security updates and the standard by which "unreasonable" self-preferencing would be defined. But perhaps most concerning is the private right of action it would create for rival firms to bring litigation. This could open the door to massive rent-seeking behavior.

For more on the benefits of self-preferencing and closed platforms, see Geoffrey A. Manne's "Against the Vertical Discrimination Presumption." For more on prior legal disputes over app store policies, see Dirk Auer's "The Epic Flaws of Epic's Antitrust Gambit." For more on the data security risks of sideloading, see Mikołaj Barczentewicz's "Privacy and Security Implications of Regulation of Digital Services in the EU and in the US."

CONTACT US

Dirk Auer
Director of Competition Policy
dauer@laweconcenter.org

Geoffrey A. Manne
President & Founder
gmanne@laweconcenter.org

ICLE International Center for Law & Economics