ACT
The App Association

Platforms and Competition

Discover the App Economy

Key Takeaways

1 Developers like ACT | The App Association members want transparency and responsive developer services in the online app marketplace.

2 It’s critical for small app companies to have trusted marketplaces with low barriers to entry to distribute their products and services globally.

3 Congress should support federal privacy and data security legislation and maintain a trusted app marketplace in the ways outlined here.

Competition Principles for a Thriving App Economy

Throughout the last several years, regulators and policymakers have been taking a close look at competition in online marketplaces. This scrutiny has put a spotlight on how the app development community works with the largest consumer-facing app stores like Apple's App Store and the Google Play store, but also platforms like Epic Systems (healthcare), Nintendo (games), and Oracle (business). Consumer-facing app stores link to mobile operating systems to form two-sided software platforms, the trusted marketplaces that connect app companies with millions of potential clients and customers across the globe. **While discussions have referenced "small developers" in the abstract, policymakers must understand that App Association member interests do not align with some large companies on the app stores seeking to lower their own distribution costs.**

Unfortunately, a tiny subset of dominant companies is lobbying for two bills that would shift distribution costs down to the smallest app makers: the American Innovation and Choice Online Act (S. 2992/H.R. 3816, 117th) and the Open App Markets Act (S. 2710/H.R. 7030, 117th). These bills fail to strike a reasonable balance between access to platforms and privacy / security, as well as prohibit many of the app store management functions App Association members want. Specifically, our members rely on:

- Customer trust in the marketplace
- Immediate distribution to hundreds of millions of customers across the globe
- Marketing through the platform
- Platform-level privacy controls
- Assistance with intellectual property (IP) protection
- Security features built into the platform
- Developer tools, including accessibility features
- Access to hundreds of thousands of application programming interfaces (APIs)
- Payment processing

Ultimately, mobile app stores represent one of an array of distribution options for app makers, and they provide a bundle of services that App Association members need. Both Congress and mobile software platforms have a role in supporting small businesses in the app economy:

For Congress

- **Support federal privacy and data security legislation.** For years, we have been advocating for Congress to enact an overarching privacy and data security framework that applies across all 50 states. Consumers must trust that app makers are collecting and processing their data responsibly and that these activities are undertaken in a secure mobile ecosystem. A federal privacy law that requires covered entities to take reasonable security measures and to honor consumer rights to access, correct, delete, and transfer personal information, with strong enforcement, would increase the trust value of mobile app stores and alternative methods of software distribution like the open internet for app developers.

- **Oppose proposals like S. 2710/H.R. 7030 and S. 2992/H.R. 3816 (117th).** These bills are designed to advantage the largest companies selling digital-only goods and services on the app stores while shifting the costs of maintaining the app stores down to the smallest sellers like App Association members. The bills would also prohibit privacy and security measures the app stores take to maintain a trusted marketplace, at a time when App Association members are seeking privacy and security requirements.

For Mobile Software Platforms

Developers want more transparency. Our member companies pay a fee to platforms for developer services, and they expect those services to meet their needs. Transparency should be a priority in a couple of key areas:

- **In the review process**. When a developer submits software for review, app stores should be transparent about how the developer can meet the app stores' requirements. Conversely, app stores must also clearly explain why certain apps are rejected and ensure the developer understands how to correct the mistakes that led to rejection.

- **For any changes to guidelines**. Some developer guideline updates are self-explanatory. But in many cases, changes to the guidelines can fundamentally alter the kinds of disclosures or relationships developers can have with their clients and consumers. For example, Apple's introduction of Privacy Nutrition Labels helped simplify privacy communications between developers and consumers but raised new questions for app makers trying to understand how to properly disclose under the new framework. Updates like this must come with developer assistance and transparency.

- Developers want responsive developer services. When a member company spots a competing app pumping up their ratings with fake reviews, usually it's a violation of the app store guidelines that should be corrected. App makers want quick resolution in cases like this, which requires substantial investment by mobile platforms in personnel and technology. Similarly, robust initial app reviews that strictly reject untenable privacy and security risks are important for app maker success.

- Proposals like S. 2992 and S. 2710, which would prohibit platform-level quality measures like these, would obviously undermine app makers' ability to rely on them.

For Mobile Software Platforms and Congress

- **Preserve access to global markets and low barriers to entry.** By offering trusted marketplaces for app makers to distribute their products and services globally, mobile software platforms contribute substantially to market conditions with low barriers to entry for entrepreneurs from diverse backgrounds to achieve global success.

- **Further global leadership on privacy and IP.** Congress and platforms must enable the strongest privacy and security protections possible against threats to Americans' privacy and IP—especially from those that originate in China.