ACT
The App Association

# Encryption and Cybersecurity

Discover the App Economy

# Key Takeaways

1. The need for updated cybersecurity legislation is most acute for small businesses like ACT | The App Association members, since up to 71 percent of cyber attacks target small companies.

2. Strong encryption standards are critical for small businesses and developers to keep their users' personal and sensitive data safe in the online marketplace.

3. Congress should address the challenges with our federal cybersecurity posture in the ways outlined here.

# Encryption and Cybersecurity

Security threats in cyberspace present complex and quickly evolving policy challenges for Congress. Recent attacks highlight the importance of timely and appropriate disclosure of cyber incidents as well as a strong infrastructure for incident, threat, and defensive measure sharing to investigate bad actors. Although the entire ecosystem would benefit from updates to cybersecurity laws, the need is most acute for small businesses like App Association members. Up to 71 percent of cyber attacks target small companies, which suffer disproportinately from successful breaches: cyber incidents cost around $4.24 million each on average. For most small companies, that cost could destroy the firm.

Our members view the protection of their users' personal information as a core responsibility and an opportunity to earn consumer trust as a competitive advantage in the marketplace. That holds especially true when the personal information at issue involves the contents of users' private communications or other sensitive information. We simply do not believe that undermining encryption—for example, to facilitate the scanning of user communications for surveillance purposes—can coexist with this principle.

At a minimum, Congress must improve the cybersecurity posture of small businesses by resisting calls to weaken encryption that protects the flow and storage of sensitive personal information, improve federal law enforcement's digital evidence capabilities, and help employers access and develop American cybersecurity talent.

## Policymakers Should Keep the Following Considerations in Mind on Encryption and Cybersecurity:

### Encryption is crucial to the digital economy

Safeguarding Americans' digital transactions, from mobile banking to healthcare to retail purchases, depends on the ability to use strong technical protection mechanisms, including encryption. Luckily, policies encouraging data encryption to combat unauthorized access to data and protect consumers already exist. For example, the National Institute of Standards and Technology (NIST) and the Department of Health and Human Services (HHS) developed standards and enforcement guidance to make encryption a functional requirement.

### Introducing backdoors to encryption harms the very groups those proposals seek to protect

Encryption is key to the privacy and security of users across the internet, and this is particularly true for members of vulnerable groups. For example, as children and families use the internet to access essential services such as education, healthcare, and even social interaction, screen time has skyrocketed. Weakening encryption undermines the trust individuals place in those services and, ironically, provides child predators and other would-be interlopers a compromised attack vector through which to more easily track and target children. Instead, Congress should enact legislation like the Ensuring National Constitutional Rights for Your Private Telecommunications (ENCRYPT) Act (H.R. 3520, 117th), which would protect encryption across the nation by prohibiting state or local laws mandating backdoors.

## Software platforms and cloud services play a key role in our cybersecurity posture

As app makers, our member companies benefit from leveraging the security features in mobile devices and their operating systems, as well as in app store vetting, which prevents malware or otherwise unsecure apps from reaching users. The vetting function is a worthwhile hurdle our member companies clear because it creates an environment in which consumers trust the apps in the store, even when they come from app makers they have never heard of—the common profile of our member companies.

We must preserve platforms' ability to perform these essential tasks by rejecting overbroad antitrust legislation that would make them illegal, such as 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).

Similarly, cloud storage and related services typically make security more accessible for smaller companies by providing built-in technical protections at lower costs and benefitting from internal threat, defensive measure, and incident intelligence from a broad customer base. It is simply more resource-intensive to maintain robust cybersecurity protections around on-premises infrastructure, especially for small companies.

## Congress can do more to protect small businesses from cyber threats

Congress should pass legislation like the Small Business Advanced Cybersecurity Enhancements Act (H.R. 4513, 117th), which designates a single federal entity, the Small Business Administration (SBA), as the cyber threat information sharing hub for small businesses based in the United States that are not otherwise under a separate information sharing framework. Enhancing information sharing by making it more accessible for small companies is especially important because they are a favorite target of cyber criminals and lack the resources to seek out obscure and expensive information sharing frameworks that larger companies commonly use.

## The cybersecurity field has a serious talent gap

With more than 500,000 unfilled cybersecurity jobs, there are not enough technically-trained professionals to meet the needs of the app ecosystem or the broader U.S. economy. Tech companies and our educational institutions work hard to train American students, entry-level workers, and mid-career professionals for the jobs of the future. As national security increasingly intertwines with defending from cyber attacks, we encourage Congress to provide resources for these educational efforts to protect commercial operators and our country's safety.