


Encryption and Cybersecurity





Security threats in cyberspace present complex and quickly evolving policy challenges for Congress. Attacks like the Change Healthcare breach 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 ACT | The App Association members. Up to 71 percent of cyberattack targets are small companies, which suffer disproportionately from successful breaches. The average cost of a breach is now **around \$4.88 million** per cyber incident for entities of any size and **\$2.98 million for small businesses**. 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 do not believe that undermining encryption—for example, to facilitate the scanning of user communications for surveillance purposes—can coexist with this principle. But don't take it from us. The **Salt Typhoon attacks** in late 2024—which took advantage of mandatory backdoor access for law enforcement built into broadband networks—illustrate that backdoors necessarily lead to compromise.

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 enforcement guidance strongly encouraging the use of encryption to meet privacy and security needs.
- **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 like the elderly, children, and busy families. Weakening encryption undermines the trust individuals place in it and, ironically, provides child predators and other would-be interlopers a compromised attack vector through which they can 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. 5311, 118th)**, 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 through 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. 2033, 118th)**.