# Encryption & Lawful Access

ACT | The App Association

Security threats in cyberspace present complex and quickly evolving policy challenges for Congress. Technology changes much faster than our statutes and regulations. In many cases, applying ill-conceived and/or outdated laws to the digital economy could impede our ability to mitigate serious and dynamic cyber threats.

Congress should resist calls to weaken encryption by mandating law enforcement access to encrypted information and instead provide incentives for cyber threat information sharing and help employers access and develop American cybersecurity talent.

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

- **Encryption protects the life and property of Americans.** Safeguarding Americans' digital transactions, from mobile banking to healthcare to retail purchases, depends on the ability to use strong technical protection mechanisms, including encryption. In 2019, identity thieves successfully targeted 14.4 million Americans, 33 percent of whom have experienced identity theft, which is more than twice the global average. 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.

- **Encryption only works if the keys are kept safe.** Unfortunately, law enforcement agencies often seek "backdoor access" to encrypted data, arguing that they should have the keys to decrypt private information. When advocates seek this kind of access, they create a more dangerous world for the citizens they are bound to protect. A report by the Center for Strategic and International Studies (CSIS) found that policymakers should first address inadequate training and digital resources for law enforcement officials. This is why we support the **Technology in Criminal Justice Act** (H.R. 5227), which requires more robust training for law enforcement investigators on the use of digital evidence.

- **The cybersecurity field has a serious talent gap.** With more than 507,924 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 work hard to train American students, entry-level workers, and mid-career professionals for the jobs of the future. As national security is increasingly intertwined with defending from cyber attacks, we encourage Congress to provide resources for these educational efforts to protect commercial operators and our country's safety.

- **Congress should resist calls to balkanize the internet.** Concerns around foreign governments' access to data on Americans has led to policy proposals ranging from banning apps with Chinese ownership to requiring reporting on the storage of data held in certain countries. For policymakers concerned about American companies complying with investigations by other nations, the good news is that American law generally outlaws such compliance in Section 2702 of the Electronic Communications Privacy Act (ECPA). To the extent concerns are focused on possible unauthorized access by other governments, those concerns only underscore the need to preserve strong encryption methods. Data storage is global and fluid, often relying on local caching to serve nearby users. American policymakers have almost universally opposed data localization requirements by foreign governments because they would disrupt this global flow of data. They should continue to resist any policies that push the internet toward a series of disconnected networks geofenced at national borders and instead encourage strong encryption to shield data from unauthorized access.