

The Secure Data Act

The **Secure Data Act** will prohibit Federal agencies from requiring that private entities design or alter their commercial information technology products for the purpose of facilitating government surveillance.

U.S. government and independent experts have extensively documented the multi-billion dollar threat posed by constant cyberattacks from criminal organizations and foreign government-sponsored hackers. The U.S. government also urges private companies and individuals to protect sensitive personal and business data, including through the use of data security technologies such as encryption. The recent proposals from U.S. law enforcement officials to undercut the development and deployment of strong data security technologies by compelling companies to build backdoors in the security features of their products work against the overwhelming economic and national security interest in better data security.

Moreover, the decision of government officials to repeatedly mislead the American public about domestic surveillance activities has resulted in an erosion of public trust. Requiring computer hardware and software companies to now create intentional gaps in their data security products to facilitate further government access to personal data will undermine the effort to restore trust in the U.S. digital economy.

Government-driven technology mandates to weaken data security for the purpose of aiding government investigations would compromise national security, economic security and personal privacy.

- **Cyber vulnerabilities weaken cybersecurity.** Once a backdoor is built in a security system, the security of the system is inherently compromised. For example, in 2005 it was revealed that an unknown entity had exploited a “lawful intercept” capability built into Greek cellphone technology and had used it to listen to users’ phone calls, including those of dozens of senior government officials.¹
- **Technology mandates thwart innovation.** Companies have less incentive to invest in the development and deployment of strong new data security technologies if they are required to compromise them from the outset.
- **Mandating weak security would further erode trust in American products and services.** Information technology companies are working to regain the trust of consumers upset by revelations of government intrusions into their personal communications. A mandate requiring companies to facilitate additional government surveillance would undermine those efforts.

¹ See Cassell Bryan-Low, “Vodafone, Ericsson Get Hung Up in Greece’s Phone-Tap Scandal,” *The Wall Street Journal*, June 21, 2006, and Vassilis Prevelakis and Diomidis Spinellis, “The Athens Affair,” *Institute of Electric and Electronic Engineers Spectrum*, June 29, 2007.