

Tech Consumers Should Not Be Forced to Sacrifice Privacy for Security | CNBC

By Gary Shapiro

July 16, 2018

Gary Shapiro, President and CEO of the Consumer Technology Association, the U.S. trade association that represents over 2,200 consumer technology companies, argues that any law that would force companies to weaken encryption would be misguided and vulnerable to government exploitation. He writes in support of the ENCRYPT Act, which forbids such laws, and argues that transparency between law enforcement and tech companies is the best way to simultaneously protect consumers' security and privacy.

We all expect privacy, especially when it comes to our phones. But how do we feel about upholding the privacy of criminals and terrorists? And what should we do if the information needed to catch or prosecute a criminal - or potentially save lives - is locked away in someone's encrypted phone?

One problem the technology industry has recently faced is the "backdoor encryption" problem - a situation where law enforcement agencies want access to information on digital and mobile devices that may be instrumental in solving a time-sensitive case. The result is a law enforcement request for a "backdoor" to devices from tech companies - a way to bypass a device's security measures and gain access to protected devices.

In June, a bipartisan team of legislators put forward the [ENCRYPT Act](#) (Ensuring National Constitutional Rights for Your Private Telecommunications). The bill, sponsored by Rep. Ted Lieu (D-CA), [would restrict](#) state and local governments from requiring backdoors to exist, and also prevent any restriction of encryption capabilities. The goal is to develop a standardized national encryption policy that protects users' privacy rights. This bill is an encouraging step forward and one supported by the Consumer Technology Association (CTA).

Source: [Tech Consumers Should Not Be Forced to Sacrifice Privacy for Security | CNBC](#)