Privacy threat? Government plans to subvert phone encryption

Anthony Hennen

April 20, 2016

If the FBI can't persuade Congress to pass legislation forcing tech companies to break their encryption for law enforcement, they'll turn to hackers.

Amy Hess, executive assistant director for science and technology, told a Congressional panel that "encrypted communications continue to pose a challenge to the American law enforcement, and to the safety of the American public," according to *Buzzfeed*.

Without a backdoor or cooperation for encryption, the FBI argues that it's more difficult to monitor suspected terrorists. The recent fight with Apple over an encrypted iPhone owned by the San Bernardino shooter ended when the agency found "an outside party" to unlock the phone.

Hess admitted that the FBI doesn't have the skills or resources to crack encryption on its own.

"I think that we really need the cooperation of industry and we need the cooperation of academia," Hess said.

That cooperation, however, undermines encryption as a concept. If tech companies have a key that bypasses encryption and security, that security is temporary. Criminals and repressive regimes will, and have, exploited security weaknesses.

The FBI and NSA have been criticized by a Foreign Intelligence Surveillance Court judge for "compliance incidents" when the agency failed to follow procedure and what the law authorized the agencies to do. Federal law enforcement agencies have repeatedly engaged in overreach and violated the privacy of law-abiding Americans. There's little reason to believe that, were they to obtain a backdoor to encryption, that abuse wouldn't continue.

Nor is it likely that agencies would limit their scope to national security cases. "National security requests to Apple more than doubled" in 2015, according to *The Verge*, and the FBI have tried to force Apple's hand in providing assistance in a drug case. Acquiesce to federal agencies on one

national security case, and they'll extend it as far as possible, regardless of their rhetoric assuring the public they will not do such a thing. Even FBI Director James Comey conceded the case would become a precedent.

"The Justice Department might not *intend* to 'set a master key loose on the land' — but the predictable consequence of mandating compliance with requests of this type will be to significantly increase the chance of exactly that occurring," Julian Sanchez, a senior fellow at the Cato Institute, wrote of the Apple case.

The government wants to cast a backdoor to encryption as compliance with the rule of law. The practical effects will make law-abiding Americans more vulnerable to hackers.

Reform Government Surveillance, an advocacy group funded by tech companies, wrote a letter to Senators Dianne Feinstein and Richard Burr that declared "We believe it is critical to the safety of the nation's, and the world's, information technology infrastructure for us all to avoid actions that will create government-mandated security vulnerabilities in our encryption systems."

Security vulnerabilities aren't only exploitable by the American government. Russia and China could make use of those backdoors as well. Encryption doesn't put users "beyond the law," as James Comey declared. It keeps their information safe, much as a lock on a front door keeps out the police and criminals alike.