Support for national commission on terrorists' use of encryption grows

Matt A. Mayer
February 19, 2016 12:45 pm | *AEIdeas*

In an editorial today on the legal battle between Apple and the Federal Bureau of Investigation (http://www.wsj.com/articles/the-fbi-vs-apple-1455840721) over creating new software code to launch a "blunt force" attack on San Bernardino terrorist Syed Rizwan Farook's iPhone, the Wall Street Journal echoed several issues covered in my report National Commission on Terrorists' Use of Technology Needed (http://www.aei.org/publication/national-commission-on-terrorists-use-of-technology-is-needed/). Specifically, the WSJ wrote:

> Nations can mandate backdoors, but there will always be some encrypted channels outside of their jurisdiction where the likes of ISIS can plot. The result would be weaker products for law-abiding consumers that leave U.S. companies less competitive with little security benefit.

REUTERS/Damir Sagolj.

> Stronger cybersecurity is more important than ever in a world of corporate espionage, millions of compromised credit-card numbers and the stolen identities at the Office of Personnel Management. Encryption may lead to fewer antiterror intercepts, though the universe of signals that can be tapped has expanded radically and on balance more secure phones are a major advance for human freedom. Ask the Chinese pastors or Russian dissidents who are targeted by authoritarian regimes and want encrypted iPhones.
>
> …
>
> Blue-ribbon commissions are usually a form of Beltway escapism, but in this case a detailed report and recommendations from leading minds in technology, law, computer science, police and intelligence could help shape a rough consensus—or at least establish a common set of facts. Such a halfway house might also help calm political tempers and marginalize the absolutists.
>
> A mature democracy—if America still is one—ought to be able to work out these crucial matters of national security through legislative deliberation. The public interest on encryption is best served with a rational debate, not the ad hoc nuclear legal exchange that the Administration is inviting.

With reports that state and local law enforcement are prepared to file similar lawsuits to compel Apple (and presumably other technology companies like

Google) to provide the "backdoor" software to them for their criminal cases, this issue will not end anytime soon. It makes the role of a national commission all the more critical in ensuring we arrive at the "worst-best" solution to this very difficult issue.

For a detailed discussion on the national commission, please read the report (https://www.aei.org/wp-content/uploads/2016/01/National-commission-on-terrorists-use-of-technology-is-needed.pdf). My AEI colleague, Claude Barfield, also wrote an extensive analysis (https://www.aei.org/publication/order-for-apple-to-unlock-iphone-raises-myriad-of-technological-and-legal-questions/) of the technological and legal issues surrounding the Apple versus FBI battle. In an earlier blog "Apple is right to fight encryption court order as Congress dithers (https://www.aei.org/publication/apple-is-right-to-fight-encryption-court-order-as-congress-dithers/)," I supported Apple's position absent "a full national commission debate on the issues [because] [i]f US companies are going to be forced to create back doors or help the federal government hack into the encrypted technology of Americans, that mandate should come from a law passed by Congress and signed by the president. It most certainly should not come from a magistrate judge in a district court in central California based on a statute from the 1700s." For a contrary AEI opinion on the legal case, see Gus Hurwitz's blog (https://www.aei.org/publication/all-apples-writs-are-belong-to-us/) in which he states that the case is really "about willful destruction of evidence, not encryption."

Full Disclosure: I should have disclosed in my earlier blog that my wife and I own 250 shares of Apple stock. Of course, like many Americans, my family also owns two Apple computers, three iPhones, an iTouch, and two iPads.