U.S.News & WORLD REPORT

Encryption Backdoor Debate Centers on Catching Stupid Criminals

Steven Nelson
September 21, 2015

Experts on both sides agree there's limited benefit from forcing search-enabling redesigns.

Technology experts and civil libertarians squared off against government officials Monday about what, if anything, should be done to address law enforcement claims that officers and agents are increasingly unable to investigate crimes and terror plots because of widespread use of powerful encryption.

The intelligence community's top lawyer, Robert Litt, conceded at a discussion hosted by the legal blog Just Security that any government mandate that technology companies make communications available to warrant-armed investigators could introduce exploitable vulnerabilities.

And Litt, a frequent contributor to public panels in the wake of whistleblower Edward Snowden's 2013 disclosures, acknowledged there's no way to completely resolve authorities' concerns as the availability and use of open-source software increases.

But, he said, "there are a lot of sloppy and stupid terrorists out there" and "something is better than nothing," especially as "people don't always choose the most secure" technologies, an observation he supported pointing to the large user base of Gmail compared to smaller email providers.

Litt said he wasn't speaking for the Obama administration, which he said is in the midst of vigorous internal discussions about the matter. The Washington Post reported last week the White House appears to be leaning against a push for legislation that would force technological backdoors.

The issue first attracted widespread attention last year when FBI Director James Comey voiced concern about what's become branded as "going dark" – after Apple announced that iPhones would come armed with encryption that allows only the user to access stored content, in addition to end-to-end encryption that secures many in-transit messages.

At a July congressional hearing, Comey suggested major Silicon Valley companies voluntarily work on a solution. "Maybe no one will have the incentive to be as creative as we need them to be without legislation," he said.

Panelist Jonathan Mayer, a scholar at Stanford Law School’s Center for Internet and Society, said he had attended meetings at well-known tech companies that have sketched a least-intrusive backdoor option using "key escrow," in which a key is stored for decryption as needed. But he said there’s vehement opposition among software engineers concerned about risks from people who aren’t court-authorized U.S. officials.

Litt, who says he was told by another tech company they hadn’t spent much time on the issue, said he’s heard of other potential ways to implement what he said was more fairly called a “front door.” An excited Mayer failed to extract from him more information. Litt said he “couldn’t possibly recite it in a coherent manner.”

Kiran Raj, senior counsel to the deputy attorney general, said the government was beginning to collect better data to quantify the problem and that collecting real-time information requires an arduous process proving “probable cause plus” before winning a judge’s approval.

Raj attempted to draw a contrast between what he called “warrant proof” encryption – through which only a user could decrypt communications – and “strong” encyrption where companies retain some information for their own purposes. Mayer retorted that "end-to-end" encryption is the actual industry-accepted term, and that Litt's use of the term "front door" is similarly an attempt to rebrand backdoor.

Wendy Seltzer, who serves on the board of the Tor Project, which operates a popular Web browser that protects user privacy, said open-source software would scuttle attempts to mandate backdoors, noting a prospective Tor user could just download a version of the software from another source.

But Georgetown University law professor Paul Ohm, the panel moderator, reiterated Litt’s contention that many criminals would not take such safeguards. “There are a lot of dumb criminals out there, a lot of them!” he said.

Seltzer said, even with universal strong encryption, “you still have all the other ways in which they are dumb.”

Cato Institute scholar Julian Sanchez rolled his eyes at the need to discuss the matter.

“This talk about smart and dumb criminals is a little crude,” he said. “The expiration date on this has passed, unless you can think of a way to make ISIS use your backdoor software.”