New privacy battle looms after moves by Apple, Google

October 1 2014, by Rob Lever

A new battle is brewing over privacy for mobile devices, after moves by Google and Apple to toughen the encryption of their mobile devices sparked complaints from law enforcement

A new battle is brewing over privacy for mobile devices, after moves by Google and Apple to toughen the encryption of their mobile devices sparked complaints from law enforcement.

The issue is part of a long-running debate over whether tech gadgets should have privacy-protecting encryption which makes it difficult for law enforcement to access in time-sensitive investigations.

FBI director James Comey reignited the issue last week, criticizing Apple and Google for new measures that keep smartphones locked down—without even the company holding the keys to unlock the data.

"What concerns me about this is companies marketing something expressly to allow people to place themselves beyond the law," the FBI chief said, warning that law enforcement may be denied timely access, even with a warrant, in cases ranging from child kidnapping to terrorism.

Former FBI criminal division chief Ronald Hosko made a similar point in an opinion piece in the Washington Post, citing a case in which the agency used smartphone data to solve a brutal kidnapping just in time to save the life of the victim.

"Most investigations don't rely solely on information from one source, even a smartphone," he said. "But without each and every important piece of the investigative puzzle, criminals and those who plan acts destructive to our national security may walk free."

Crypto Wars 2.0

Observers who follow privacy and encryption say they have seen this debate before.

In the mid-1990s, as the Internet was gaining traction, the government pressed for access to digital "keys" to any encryption software or hardware, before abandoning what ended up being a futile effort.

"This is Crypto Wars 2.0," says Joseph Hall of the Center for

Democracy and Technology, a digital rights group active in both campaigns.

FBI director James Comey reignited the issue last week, criticizing Apple and Google for new measures that keep smartphones locked down

Today, "the main difference is that phones are increasingly deeply personal, containing much more daily life and interaction than a desktop from the 1990s" Hall said.

Hall argued that giving law enforcement access requires companies to "engineer vulnerabilities" which could be exploited by hackers or others.

"There's no way to tell the difference between a good guy and bad guy when they walk through the back door," he said.

Cindy Cohn of the Electronic Frontier Foundation says the FBI has been making these arguments since 1995, with the same flawed logic.

"We've seen this movie before," Cohn said.

"Regulating and controlling consumer use of encryption was a monstrous proposal officially declared in 2001," she said in a blog post. "But like a zombie, it's now rising from the grave, bringing the same disastrous flaws with it."

In 2013, before the revelations of massive surveillance from leaked National Security Agency documents, the FBI called for broader authority to capture mobile communications which fall outside traditional surveillance, such as Skype and Google Hangouts.

But civil liberties activities say leaked NSA documents suggest that contrary to FBI claims made last year, the government has many tools at its disposal.

"There are an increasing number of places where we leave our digital trails," Hall said, including in the Internet cloud, where it can be accessed with a court order.

The issue is part of a long-running debate over whether tech gadgets should have privacy-protecting encryption which makes it difficult for law enforcement to access in time-sensitive investigations

No back doors

Jennifer Granick, director of civil liberties at the Stanford University Center for Internet and Society, said the FBI argument overlooks the fact US tech firms must compete in the global marketplace.

"Global customers do not want backdoored products any more than Americans do, and with very good reason," Granick writes on the "Just Security" blog.

"Authoritarian countries like Russia, China, the United Arab Emirates, Sudan, and Saudi Arabia want to censor, spy on, and control their citizens' communications. These nations are just as able to make

demands that Apple and Google decrypt devices as the FBI is, and to back up those demands with effective threats."

On balance, she said, "the public is more secure, not less secure, with the wide use of strong cryptography—including cryptography without back doors."

Mike Janke, chief executive of the firm Silent Circle which makes the fully encrypted Blackphone, said the FBI is making a "false cry" against Google and Apple because the law enforcement agency can easily gain access to a phone—through a carrier tap, or location tracking, for example.

Greater privacy, Janke said, comes from the harder encryption on Blackphone, but law enforcement can still track a user's location as long as the battery is inside.

While a small number of people may use encryption for nefarious purposes, Janke said, "do you sacrifice the privacy and trade secrets of everyone else because of that?"