Written by **Bob Adelmann** on September 28, 2014

Apple, Google Encryption Moves Enrage FBI Director Comey

A week after smartphone makers Apple and Google announced software that now makes their phones impervious to government snooping, FBI Director James Comey expressed outrage, claiming that he could simply not understand why these two companies would "market something expressly to allow people to place themselves above the law." He added: "There will come a day when it will matter of great deal to the lives of people … that we be able to gain access [to that private information]."

Of course, such information is, or should be, protected under the Fourth Amendment to the Constitution.

What the new software means is that law enforcement officials will have to go back to the old way of investigating crime and turning up incriminating evidence. They will still be able to seek records of calls or texts from cellular carriers, eavesdrop on conversations and, based on the cell towers used, determine the general locations of suspects. They also will be able to access private data deliberately or unintentionally backed up on remote cloud services. And law enforcement agencies continue to have the capability of installing malicious software onto smart phones, turning them into virtual spies on the behavior of their owners.

On its website Apple noted: "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government [search] warrants for the extraction of this data from devices in their possession running [operating system] iOS 8."

But both companies will still have the ability, and the legal responsibility, to turn over any user data stored elsewhere, such as on cloud services, which typically include backups of photos, videos, e-mail communications, and music collections. Users wishing to prevent law enforcement from going after that data will have to adjust their personal settings that block that data from flowing to the cloud.

Christopher Soghoian, a software technology expert for the American Civil Liberties Union (ACLU), was delighted about the new software:

> This is a great move. Particularly after the Snowden disclosures, Apple seems to understand that consumers want companies to put their privacy first.
>
> However, I suspect there are going to be a lot of unhappy law enforcement officials.

Another of those unhappy law enforcement officials is Ronald Hosko, a former investigator for the FBI, who labeled the encryptions by Apple and Google "problematic," adding that it will make life more difficult for law enforcement to collect key evidence. He declared that "our ability to act on data [stored

in these devices] is critical to our success" in preventing and solving crimes.

For more than three years, Google's Android device has had encryption capability, although it was difficult to engage. In Android's latest iteration, that encryption will now be enabled automatically right out of the box so that, as Android spokeswoman Nikki Christoff said, "You won't even have to think about turning it on."

These moves reflect a seismic groundswell of outrage against the federal government's invasions of privacy which were first exposed by Edward Snowden, a computer professional who leaked classified information from the National Security Agency (NSA). Craig Timberg, writing in the *Washington Post*, called it "a part of a broad shift by American technology companies to make their products more resistant to government snooping" in the aftermath of the Snowden revelations.

It also makes largely redundant the Supreme Court's unanimous decision in June, in *Riley v. California*, which concluded that "police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." Writing for the unanimous court, Chief Justice John Roberts noted:

> Modern cell phones are not just another technological convenience. With all they contain and in all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.

He added:

> The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, Rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers.

Prior to that decision, law enforcement officials were able to use the doctrine of SITA — Search Incident To Arrest — a broad exception carved out of the Fourth Amendment allowing police to seize and download information from smart phones obtained during an arrest without the need for getting a search warrant in advance.

As this unbreakable encryption technology spreads across the vast array of Apple products and, more slowly, into Google's previous iterations of its Android products, it will continue to reflect a groundswell of pushback against the surveillance state.

The National Security Agency, unfortunately, will be only slightly inconvenienced by either the *Riley* decision or the new technology announced by Apple and Google. NSA agents will continue to hoover citizens' personal data and store it in vast digital warehouses for future use at their convenience. It's going to take far more than encryption technology to protect Americans from the NSA.

Nevertheless, this decision is an important victory for privacy, even if it is not an all-important one.

A graduate of Cornell University and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at www.LightFromTheRight.com, primarily on economics and politics. He can be reached at badelmann@thenewamerican.com.*

Related article:

[Supreme Court Bans Warrantless Cellphone Searches]