ANTI WAR.COM
Your best source for antiwar news, viewpoints, and activities

Law Enforcement Mourns Apple’s Tighter Security Standards

By Lucy Steigerwald

October 2, 2014

On September 25, the head of the Federal Bureau of Investigation (FBI) James B. Comey criticized Apple’s plans to update their operating system to exclude any kind of so-called backdoor for law enforcement access to encrypted data on Apple devices.

Comey, like a true government official, urged people to think of the children if government officials were not allowed to access any and all encrypted information. The director said that new Apple products would endanger victims in, say, kidnapping cases. And well, what’s a privacy safeguard in the face of such a compelling hypothetical? The children will be in danger if Apple and its users are too militant about this. Comey is not alone in this attitude. In response to the news, Chicago police detective John J. Escalante unashamedly said, "Apple will become the phone of choice for the pedophile." This is the familiar refrain that those who value privacy must love criminals, which has echoed so loudly since 9/11. Terrorists, no doubt, will be picking up Apple phones as well.

As the Cato Institute’s Julian Sanchez writes, in the early days of the commercial internet, government urged tech people to include "safeguards" so that data could be accessed if deemed necessary to various investigations. Thankfully, we got our free-wheeling internet, and our well-encrypted tech instead.

Today, with fear of terrorism as an endless motivation for myriad government overreaches, the FBI in particular has been stressing that the problem of going dark is a serious one.

Going dark is when law enforcement surveillance tools cannot keep up with technology’s encryption muscle, or with other technological weasel moves meant to evade peeping outsiders. There’s a lot of web out there, from the Tor Project to the late, lamented illicit ebay Silk Road, which is anonymous – or as much as humanely possible – and is therefore seen as suspect by law enforcement. Users of Tor, which hides your IP address, have been flagged by the National Security Agency (NSA) as being up to no good. A desire for privacy is suspect.

Another problem with FBI Director Comey’s statement is its technological arrogance. Law enforcement and other government agencies may employ tech-savvy employees (ask Edward Snowden), but they are not the people inventing this stuff. There are risks – beyond violations of basic principles of privacy rights – to mandating that inventors include ways to access information that is meant to be secure.

For one, allowing government access – even qualified access – inherently makes data more hackable by outsiders. Everyone wants to build software that is safe from outside attacks. You can’t build software that knows it’s someone with a legal search warrant poking around, not a a would-be identify thief. Innocent people’s property and privacy rights are less secure thanks to law enforcement’s need to catch various criminals.

Even if the NSA, FBI, and other groups wouldn’t dream of suggesting that they are excessive in their stomping on privacy rights, they would acknowledge the existence of more repressive regimes across the globe. Citizens in these nations very lives might depend on keeping communications and information secret. Google, Yahoo!, and other tech companies have been criticized in the past for acquiescing to pressure from China to identify a dissident in the latter’s case, and have a Great Firewall-ready version of Google in the former. As Timothy B. Lee wrote at Vox, the UAE and other countries have also asked Blackberry – known for strong encryption – to hand over data. Why take away a company’s option of saying, "sorry, we actually can’t help you with that, Mr. Dictator"?

Police and federal law enforcement can wiretap, use stingrays, or tower dumps, or other methods of tracking and surveillance on crime suspects, or endangered victims. In a recent Washington Post article, former FBI official Ronald Hosko wrote, "We shouldn’t give [criminals] one more tool" to get away with their shady endeavours. The same can be said of a government famished for data, and which criminalizes too many things.

Violent crimes like the kidnapping example Hosko uses – whose victim still would have been saved in a world of fully encrypted iPhones, turns out – are rare. Government spying, as we have learned so keenly in the last year and a half, is much more common.

The government simply doesn’t need yet another method of getting to us, especially not when that method arrogantly presumes that government policy can invent things. The brilliant little machines we now use to to do everything from watch movies, to navigate the country, to find dates were not invented by decree from above. Companies need freedom to build their systems the way they see fit. It is not law enforcement’s job to mandate any of their decisions, but to try and keep up as best they can.

Not to mention, as Sanchez noted, Apple’s full encryption is not a novelty. That their devices will be this way by default is what is notable. One needn’t depend on customers – regular, or criminal, depending – to have the know-how to do this. Apple will now do it for them, which is what is ticking law enforcement off so much.

Engineers who are closing loopholes and hatches into which government spooks can creep should be saluted for ignoring Uncle Sam’s data addiction, as well as their hand-wringing over pedophiles and kidnappers, terrorists and drug smugglers, around every corner. Privacy is a good for its own sake. Most people want to keep theirs just because.