REAL CLEAR POLITICS

Encryption Is the Key

Carl M. Cannon

June 28, 2018

Although the bad blood between President Trump and James Comey helped shape our current contentious political environment, on one highly charged policy issue both men were in complete agreement during the brief time Comey served under Trump. That issue relates to cybersecurity and the pitched battle between law enforcement and the tech industry over encryption.

The president and the former FBI director have been equally vehement in their denunciation of Silicon Valley tech giants for building encrypted software code that protects users of computers and mobile phones from intrusion -- even from law enforcement officials pursing criminals.

Neither man, however, has changed many minds.

This issue burst into public consciousness after the 2015 mass murder in San Bernardino, Calif., by Muslim extremists Syed Rizwan Farook and his wife. In the name of ISIS, they opened fire at an office Christmas party, killing 14 of Farook's colleagues. Endeavoring to learn if the couple had co-conspirators, the FBI tried for weeks to access the wife's iPhone. But the investigating agents couldn't get past its advanced encryption features.

Although the bureau eventually found a work-around – it hired hackers to break into the phone at a cost of $900,000 to taxpayers – Apple's unwillingness to lend a hand disgusted Jim Comey, and many other Americans, including presidential candidate Donald Trump. "To think that Apple won't allow us to get into her cellphone," Trump said. "Who do they think they are?"

Even before that tragic case, Comey raised the specter of the government compelling Apple and Google, among others, to provide backdoors to their systems. Encryption, he said in a 2014 speech at the Brookings Institution, was being used by "predators" and "bad guys" and was leading the country "to a very dark place."

"Congress might have to force this on companies," Comey added. "Maybe they'll take the hint and do it themselves."

Silicon Valley executives and thought leaders in the tech field most definitely did not take that hint, and in his 2018 tell-all book, Comey was still lashing out at them. Apple's "appalling" intransigence "drove me crazy," he wrote, adding that the tech executives enjoying lives of luxury in sunny California "don't see the darkness the FBI sees."

The rebuttal from the tech industry in general -- and Apple, in particular -- has been consistent now for nearly two decades. Those who want to crack open their systems, they believe, are actually the ones in the dark.

"We have great respect for the professionals at the FBI, and we believe their intentions are good," Apple CEO Tim Cook wrote in an open letter to Apple's customers in February 2016. "Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone."

Although the explanations can get pretty technical, industry execs such as Cook – along with most cybersecurity experts -- believe that the problem is basically two-fold. First, creating security systems with hidden encryption keys, or "backdoors," in them is inherently inefficient and exponentially increases the likelihood of software bugs. Second, and more directly on point: They believe that the only certainty with an encryption key is that ultimately it will fall into the hands of the "bad guys" Comey referenced.

"As a practical matter, you can't design a system that can be breached without weakening the central security for everyone," says Julian Sanchez, a Cato Institute senior fellow who studies the nexus between technology and privacy. In his view, creating a security system that is designed to be broken into invariably *lessens* security – and is essentially an oxymoron.

This view is prevalent in the tech community. Earlier this month, The Washington Post surveyed a panel of 100 digital security experts about the FBI's contention that its inability to access encrypted mobile phones has compromised national security. Seventy-two percent thought the opposite was true.

"The idea of the 'golden key' – access that only the good guys can use -- is a myth," Jamie Winterton of Arizona State University's Global Security Initiative, told the Post. "Once that access had been created, it could be used by the FBI -- or it could be used by foreign adversaries."

"The idea of the 'golden key' – access that only the good guys can use – is a myth."

Jamie Winterton, Arizona State University's Global Security Initiative

This is not a new insight. Nor is the desire new on the part of various national security agencies and other law enforcement officials to chip away at it. In the late 1990s, as these technologies were expanding exponentially and the tech industry was turning to encryption as a deterrent to massive data breaches, the battle lines were drawn. The U.S. government and some other Western intelligence services had proposed deploying data requiring third-party encryption keys. When word of this reach Silicon Valley, everyone from the programming nerds to company officers in the executive suites was alarmed.

In January 1997, at Sun Microsystems in Menlo Park, Calif., an ad-hoc group of privacy experts, industry officers, and academics began to study the problem. The fruit of their labor was a May

27, 1997 report now known as “Keys Under Doormats,” which concluded that what law enforcement in this country thought it wanted would actually make its work much harder.

“The deployment of key-recovery-based encryption infrastructures to meet law enforcement’s stated specifications will result in substantial sacrifices in security and greatly increased costs to the end user,” it concluded.

In many ways, the argument has been stalemated ever since. No sooner had James Comey finished his book tour than Apple announced something that would have driven him crazy all over again. The company said earlier this month that as part of its next software update, an hour after iPhone users lock their phones, a port known as “Lightning,” located at the bottom of the phone, will automatically be disabled. The typical Apple user won’t notice, but cybersecurity experts working for law enforcement certainly will: Lightning may have been the closest thing to a key under the doormat, a port Apple fears could be used by cyber sleuths – not all of whom have good intent – as an extraction tool.

In a statement announcing the change, Apple made a point of saying that its goal wasn’t to thwart law enforcement. It was to thwart criminals. “We have the greatest respect for law enforcement, and we don’t design our security improvements to frustrate their efforts to do their jobs,” the company said in a written statement. “We’re constantly strengthening the security protections in every Apple product to help customers defend against hackers, identity thieves and intrusions into their personal data.”

But if the terms of the debate over this topic are not new, the historical context is not the same as it was in 1997. What altered the conversation, at least for some people, was 9/11. If encryption keys or “back doors” could help prevent a similar attack, they ask, isn’t it worth a certain level of inconvenience?

“I've been concerned about the tech industry taking steps to encrypt communications, develop apps, and design other technology that will defeat the lawful, legitimate, and necessary efforts of law enforcement to collect and exploit data that they're entitled to,”

Ronald Hosko, former FBI assistant director, told RealClearPolitics. “The FBI [fears] that they'll be blind to terrorist plots and criminal conspiracies because of encryption.”

Hosko, who is now president of the Law Enforcement Legal Defense Fund, says that agents have persuaded judges to grant search warrants and court orders, but that increasingly the data they seek is not retrievable. Hosko believes Congress is shirking its duty to exercise oversight over tech firms, which in turn are using “privacy” as a pretext to persuade their customers to ignore the threat to public safety.

“But we know that bad actors are taking advantage of law enforcement blind spots and it's only a matter of time until there’s a significant attack, with significant loss of life -- and with sufficient public outrage and finger-pointing, they'll reevaluate their positions,” he added. “Typically, America needs a crisis to act decisively. I hope that’s not what it takes to drive change here.”