Trump administration ramps up campaign to abolish strong data encryption in aftermath of Pensacola terror shooting

Kevin Reed
21 January 2020

The Trump administration is using a Justice Department investigation into the terrorist shooting at the Pensacola Naval Base on December 6 to advance its campaign to abolish end-to-end encryption and enable law enforcement unfettered access to personal data on consumer electronics devices.

At a press conference on January 13, Attorney General William Barr demanded that Apple provide the US Department of Justice (DOJ) with access to two iPhones used by the gunman, Second Lt. Mohammed Saeed Alshamrani. A cadet in the Saudi Air Force who was training with the American military, Alshamrani killed three sailors and wounded eight others in a shooting rampage in a training facility at the Pensacola base.

Alshamrani was shot and killed by sheriff's deputies who arrived on the scene an hour after he opened fire with a 9mm Glock handgun. The DOJ has characterized the incident as an act of terrorism motivated by jihadist ideology.

In his press conference, Barr said, "We have asked Apple for their help in unlocking the shooter's phones. So far, Apple has not given any substantive assistance." Apple issued its own statement later that day, however, disputing Barr's claim. "We reject the characterization that Apple has not provided substantive assistance in the Pensacola investigation," the tech giant stated. "Our responses to their many requests since the attack have been timely, thorough and are ongoing."

On the day of the shooting, Apple provided the FBI with "a wide variety of data," including the iCloud backups of the shooter's data. Apple said that it gave support to investigators. "We responded to each request promptly, often within hours, sharing information with FBI offices in Jacksonville, Pensacola and New York," it declared, adding, "The queries resulted in many gigabytes of information that we turned over to investigators. In every instance, we responded with all of the information that we had."

Pointing to the scripted nature of Barr's press conference, Apple also noted, "The FBI only notified us on January 6th that they needed additional assistance—a month after the attack occurred. Only then did we learn about the existence of a second iPhone associated with the investigation and the FBI's inability to access either iPhone."

Barr eventually got around to explaining the reason for his public criticism of Apple, "This situation perfectly illustrates why it is critical that the public be able to get access to digital evidence once it has obtained a court order based on probable cause. We call on Apple and other technology companies to help us find a solution so that we can better protect the lives of the American people and prevent future attacks."

The "solution" that Barr is demanding from the tech industry is a halt to end-to-end encryption implementation in consumer electronics devices or—what amounts to the same thing—granting the state backdoor access to all encrypted data and locked and password-protected devices with a special universal key.

Speaking to reporters after the press conference, Barr said, "We're seeing an increasing number of these cases and it's becoming a grave problem. We don't want to get into a world where we have to spend months and even years exhausting efforts when lives are in the balance. We should be able to get in once we have a warrant that establishes that criminal activity is probably underway."

In other words, Barr is using the events in Pensacola as justification for abrogating fundamental privacy rights of the public. The mentioning of "once we have a warrant" is for PR purposes only, since everyone is well aware that the state is eavesdropping on and gathering their electronic communications without permission or authorization from any court.

In a statement to *Recode,* Apple explained its position on end-to-end encryption, "We have always maintained there is no such thing as a backdoor just for the good guys. ... Backdoors can also be exploited by those who threaten our

national security and the data security of our customers. Today, law enforcement has access to more data than ever before in history, so Americans do not have to choose between weakening encryption and solving investigations. We feel strongly encryption is vital to protecting our country and our users' data."

President Trump took to social media a day later to ramp up the pressure on Apple and other tech firms defending consumer-level encryption. He tweeted, "We are helping Apple all of the time on TRADE and so many other issues, and yet they refuse to unlock phones used by killers, drug dealers and other violent criminal elements. They will have to step up to the plate and help our great Country, NOW!"

The present public denunciations of Apple are an intensification of the campaign by the FBI, DOJ and White House going back to the Obama presidency and the terrorist shootings in San Bernardino, California on December 2, 2015. During that investigation into the rampage by Syed Rizwan Farook and Tashfeen Malik that killed 14 and wounded 22, the FBI demanded that Apple unlock an iPhone that belonged to Farook.

When Apple refused, the Obama administration, under the direction of Attorney General Loretta Lynch and FBI Director James Comey, attempted to skirt the constitutional issues involved by getting a US magistrate judge to issue a court order under the All Writs Act of 1789 that would compel the company to unlock the phone. When Apple vowed to challenge the writ in court, the FBI contracted with a third-party firm called Cellebrite to gain access to the iPhone contents by tethering it to a personal computer.

Last July, Attorney General Barr gave a speech at a cyber security conference in New York City where he said the DOJ would pursue either a legal challenge or legislation that will force the tech industry to provide backdoor access to encryption of consumer electronics devices and software apps. Inverting the democratic principle of the Fourth Amendment, Barr argued that "individual privacy" protections against unreasonable searches and seizures should "always be" balanced against "public safety."

That the recent public statements by Barr and Trump are part of a political campaign to build support for abolishing end-to-end encryption is proven by other technical details about the Pensacola shooter's iPhones.

According to *Wired*, the reason Cellebrite was able to access the locked San Bernardino shooter's smartphone in 2015 was because it was an iPhone 5C running the iOS 9 operating system, which had security vulnerabilities. In response, Apple began to modify the operating system of iPhones and, in 2017 with iOS 11, the type of data protection circumvention used in 2015 had been specifically blocked.

However, hackers once again caught up to the 2017 security changes, with Cellebrite announcing publicly that it had cracked user data protections for all Apple mobile devices up to those with iOS 12.3, and other researchers discovered hardware security flaws that enable access to any Apple device released between 2011 and 2017.

It has been determined that both of the Pensacola shooters' phones—an iPhone 5 and an iPhone 7—fall within these parameters. As explained by *Wired*, "Alshamrani did attempt to physically destroy both by shooting and smashing them, but attorney general William Barr has said that the FBI's Crime Lab was able to 'fix both damaged phones so that they are operational.'"

What this means is either the statements of Barr and Trump that Apple has refused to unlock the Pensacola shooter's phones are irrelevant, or Barr's statement that the iPhones have been fixed is false.

As Matthew Green, a cryptographer from Johns Hopkins, told *Wired*, "As far as we know, law enforcement has a number of workable options for unlocking phones, particularly older phones like these. It's not clear to me why those tools wouldn't work against these phones, but it's possible that it's related to the deliberately inflicted physical damage. If that's the case, then it seems that the FBI doesn't have an Apple problem, it has a bullet problem."

According to a report in the *Washington Post*, the White House campaign is making headway in Washington, D.C. with "an increasing willingness on Capitol Hill to pass legislation requiring tech companies to make their encrypted devices accessible to law enforcement." In an interview with the *Post*, Assistant Attorney General John Demers said, "I've never seen the atmosphere here in D.C. to be so conducive to passing some kind of encryption legislation or lawful access legislation as it is today."

During a Senate hearing in December, Judiciary Committee Chairman Lindsey Graham (Republican of South Carolina) said that the Silicon Valley tech firms had to build access into their phones, adding, "My advice to you is to get on with it because this time next year, if we haven't found a way that you can live with, we will impose our will on you."