US government uses Pensacola shooter's alleged ties to Al Qaeda to renew attack on end-to-end encryption

By Kevin Reed
20 May 2020

The US Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) ratcheted up the attack on end-to-end encryption of consumer electronic and mobile devices on Monday during a virtual press conference to review developments in the investigation of the Naval Air Station shooting in Pensacola, Florida last December.

Attorney General William Barr and FBI Director Christopher Wray both specifically denounced Apple, Inc. for refusing to unlock the encrypted contents of the two iPhones belonging to Second Lieutenant Mohammed Alshamrani, a member of the Saudi air force, who killed 3 and wounded 8 in a Navy classroom before being fatally shot by law enforcement on December 6, 2019.

The US officials reported that, through their own decryption efforts bypassing Apple's built-in device security, they found that Alshamrani was a longtime affiliate of Al Qaeda. As Wray stated, "The evidence we've been able to develop from the killer's devices shows that the Pensacola attack was actually the brutal culmination of years of planning and preparation by a longtime AQAP associate." AQAP stands for Al Qaeda of the Arabia Peninsula.

A statement published by the Justice Department said, "The phones contained important, previously-unknown information that definitively established Alshamrani's significant ties to Al Qaeda in the Arabian Peninsula (AQAP), not only before the attack, but before he even arrived in the United States. The FBI now has a clearer understanding of Alshamrani's associations and activities in the years, months, and days leading up to the attack."

Barr claimed that the evidence gathered from Alshamrani's phone enabled the US government to carry out a counterterrorism operation in Yemen "targeting an operative, one of the overseas associates" and that the information "already proved invaluable in protecting the American people."

Although little details of the alleged "significant ties" and "associations and activities" of Alshamrani with AQAP were revealed, Barr and Wray moved quickly to the real purpose of their press conference: to attack Apple's defense of end-to-end encryption and refusal to provide law enforcement with a back door into encrypted personal data and communications on mobile devices.

In his remarks, Barr said that the iPhones were crucial to their investigation of the shooter, but they were locked. He said, "Apple has made a business and marketing decision to design its phones in a way that only the user can unlock the contents no matter what the circumstances. In cases like this when the user is a terrorist, or in other cases where the user is a violent criminal, a human trafficker or a child predator, Apple's decision has dangerous consequences for public safety and national security and is, in my judgement, unacceptable."

Barr then went on to say that there is no reason why Apple cannot design its consumer products and apps to "allow for law enforcement access when permitted by a judge." Significantly, Barr pointed to the collaboration of Apple and other US manufacturers with "authoritarian regimes when it suits their business interests" and referenced both China and Russia as examples of countries where Apple has cooperated with undemocratic government surveillance.

In his remarks, Wray said that FBI agents had worked

for months to break into Alshamrani's phones and added, "The magnitude of the challenge they faced is hard to overstate. We received effectively no help from Apple. We canvassed every partner, and every company, that might have had a solution to access these phones. None did, despite what some claimed in the media."

The claims that Apple provided "no help" to the Justice Department have been made by authorities since the immediate aftermath of the Pensacola shooting. However, Apple has maintained that "within hours" the company provided everything requested by the investigators including the shooter's unencrypted iCloud backups, account information and transactional data.

Meanwhile, Apple has argued that the encryption and other security features on its devices, "protect millions of users and our national security." As maintained by all of the major Silicon Valley tech firms, the creation of backdoor access undermines the entire system by making every device vulnerable to malicious cyberactivity.

Along with the specious claim that end-to-end encryption hinders important police work against "violent crimes" and "terrorism," Barr complained that the four-month effort by the FBI to decrypt Alshamrani's phones was very expensive and cost "large sums of taxpayer dollars to obtain evidence that should have been quickly accessible when we obtained the court orders"

Finally, Barr revealed that the endgame of the Trump administration is now to pass laws in the US that ban encryption on consumer devices. "The bottom line: our national security cannot remain in the hands of big corporations who put dollars over lawful access and public safety. The time has come for a legislative solution."

Behind the elaborate presentation of photos of the shooter's two iPhones and other images of notes found on the device, is the increasing effort to remove the barrier that end-to-end encryption places in the path of the US police and intelligence state from gaining unrestricted access to everyone's mobile device communications and contents at will.

As explained by Brett Max Kaufman, a senior staff attorney at the American Civil Liberties Union, "Every time there's a traumatic event requiring investigation into digital devices, the Justice Department loudly claims that it needs backdoors to encryption, and then quietly announces it actually found a way to access information without threatening the security and privacy of the entire world. The boy who cried wolf has nothing on the agency that cried encryption."

As has been the case in every instance of terrorism beginning with the attacks of September 11, 2001, the US government has exploited these violent attacks to advance imperialist war aims abroad and attack the democratic rights of the people at home.

No one should take at face value the claims about the supposed decryption of Alshamrani's iPhones and uncovering of evidence about his association with Yemeni terrorists. This is especially true given that a good number of CIA and State Department officials have the contact information of Al Qaeda members in their mobile phone address books as part of the American regime-change operations in the Middle East and Africa.

The conflict between the tech monopolies and the US government over consumer device encryption is not going to be resolved in favor of democratic rights. The ability to stop unfettered surveillance of the public—whether in the form of electronic eavesdropping on web browsing activity, facial recognition databanks or geolocation tracking—depends upon the independent struggle of the working class to defend democratic rights in the fight for socialism against the capitalist system.