FBI again finds itself unable to unlock a gunman's cellphone

November 8 2017, by Sadie Gurman

The Texas church massacre is providing a familiar frustration for law enforcement: FBI agents are unable to unlock the gunman's encrypted cellphone to learn what evidence it might hold.

But while heart-wrenching details of the rampage that left more than two dozen people dead might revive the debate over the balance of digital privacy rights and national security, it's not likely to prompt change anytime soon.

Congress has not shown a strong appetite for legislation that would force technology companies to help the government break into encrypted phones and computers. And the fiery public debate surrounding the FBI's legal fight with Apple Inc. has largely faded since federal authorities announced they were able to access a locked phone in a terror case without the help of the technology giant.

As a candidate, Donald Trump called on Americans to boycott Apple unless it helped the FBI hack into the phone, but he hasn't been as vocal as president.

Still, the issue re-emerged Tuesday, when Christopher Combs, the special agent in charge of the FBI's San Antonio division, said agents had been unable to get into the cell phone belonging to Devin Patrick Kelley, who slaughtered much of the congregation in the middle of a Sunday service.

"It highlights an issue you've all heard about before. With the advance of the technology and the phones and the encryption, law enforcement is increasingly not able to get into these phones," Combs told reporters, saying the device was being flown to an FBI lab for analysis.

Combs didn't identify the make or model, but a U.S. official briefed by law enforcement told The Associated Press it was an Apple iPhone.

"We're working very hard to get into that phone, and that will continue until we find an answer," Combs said.

Combs was telegraphing a longstanding frustration of the FBI, which claims encryption has stymied investigations of everything from sex crimes against children to drug cases, even if they obtain a warrant for the information. Agents have been unable to retrieve data from half the mobile devices—more than 6,900 phones, computers and tablets—that they tried to access in less than a year, FBI Director Christopher Wray said last month, wading into an issue that also vexed his predecessor, James Comey. Comey spoke before Congress and elsewhere about the bureau's inability to access digital devices. But the Obama White House never publicly supported legislation that would have forced technology companies to give the FBI a back door to encrypted information, leaving Comey's hands tied to propose a specific legislative fix.

Security experts generally believe such encryption backdoors are a terrible idea that could expose a vast amount of private, business and government data to hackers and spies. That's because those backdoor keys would work for bad guys as well as good guys—and the bad guys would almost immediately target them for theft, and might even be able to recreate them from scratch.

Deputy Attorney General Rod Rosenstein took aim at Silicon Valley's methods for protecting privacy during a speech last month, saying

Trump's Justice Department would be more aggressive in seeking information from technology companies. He took a harder line than his predecessors but stopped short of saying what specific steps the administration might take.

Washington has proven incapable of solving a problem that an honest conversation could fix, said David Hickton, a former U.S. attorney who now directs a cyberlaw institute at the University of Pittsburgh.

"We wait for a mass disaster to sharpen the discussion about this, when we should have been talking about it since San Bernardino," he said. "Reasonable people of good will could resolve this problem. I don't think it's dependent on the political wins or who is the FBI director. It's begging for a solution."

Even so, the facts of the church shooting may not make it the most powerful case against warrant-proof encryption. When the FBI took Apple to court in February 2016 to force it to unlock the San Bernardino shooter's phone, investigators believed the device held clues about whom the couple communicated with and where they may have traveled.

But Combs didn't say what investigators hoped to retrieve from Kelley's phone, and investigators already have ample information about his motive. Authorities in Texas say the church shooting was motivated by the gunman's family troubles, rather than terrorism, and investigators have not said whether they are seeking possible co-conspirators.

Investigators may have other means to get the information they seek. If the Texas gunman backed up his phone online, they can get a copy of that with a legal order—usually a warrant. They can also get warrants for any accounts he had at server-based internet services such as Facebook, Twitter and Google.

In the California case, the FBI ultimately broke into the phone by paying an unidentified vendor for a hacking tool to access the phone without Apple's help, averting a court battle.

The FBI has not yet asked Apple for help unlocking Kelley's phone, according to the U.S. official, who was not authorized to discuss the case and did so on condition of anonymity. Apple did not immediately return calls seeking comment.

Former federal prosecutor Joseph DeMarco, who filed a friend of the court brief on behalf of groups that supported the Justice Department against Apple, said he was hopeful the case would spur fresh discussion. If not by itself, he said, the shooting could be one of several cases that prompt the Justice Department to take other technology companies to court.

"Eventually, the courts will rule on this or a legislative fix will be imposed," he said. "Eventually, the pressure will mount."