‘Apple has to help us’ — Trump, Barr turn up heat on encryption fight

Shannon Tracy

January 23, 2020

The demands by Trump and his attorney general are raising expectations of a new push for legislation or a precedent-setting court ruling to compel Silicon Valley to give in — renewing a decades-old fight with global implications for digital security and physical safety. And while some administration officials are urging caution, Barr’s argument has carried the day so far.

Barr’s rhetoric is “probably a prelude to more litigation,” said Stewart Baker, a former NSA general counsel and Homeland Security official. “He wants to make sure he’s making DOJ’s case in public, not just in court.”

In a fraught environment for the tech community, in which lawmakers of both parties routinely bash the companies’ status and power, close observers said it was no surprise that Barr chose a terrorist attack on a military base to highlight the rising availability of uncrackable encryption. Cybersecurity experts, civil-society activists and former law enforcement and intelligence officials told POLITICO they see the attorney general’s focus on the Pensacola shooting as a strategic move aimed at influencing undecided lawmakers, judges and voters.

“It is entirely theater for the court of public opinion,” said Nicholas Weaver, a senior security researcher at the University of California, Berkeley.

Law enforcement advocates have demanded since the 1990s that creators of encrypted products install “backdoors” that would let law enforcement agencies unscramble the data after obtaining a search warrant. But privacy supporters and security experts say spies, hackers and authoritarian regimes would inevitably exploit those holes as well, endangering everyone’s safety — especially human-rights activists, dissidents and other vulnerable populations. And companies like Apple have moved in the opposite direction — creating encryption safeguards so tight that not even their developers can undo them.

Former President Barack Obama, who openly courted support from Silicon Valley, offered comparatively measured rhetoric about encryption in 2016 after Apple refused to help unlock an iPhone used by a mass shooter in San Bernardino, Calif. But Trump has repeatedly attacked Apple over the years for its use of encryption. And while some Obama advisers worried about then-FBI Director James Comey’s crusade against warrant-proof encryption, there is no sign that Trump aides have sought to restrain Barr or FBI chief Christopher Wray in their demands for backdoors.

Trump has also shown an eagerness to take on Silicon Valley over myriad issues, including allegations that tech companies are biased against conservatives — although he has sought to

form personal bonds with executives such as Apple CEO Tim Cook and Facebook CEO Mark Zuckerberg.

“There is no question that the current administration is more willing to take on the encryption fight than the prior one,” said Jamil Jaffer, a Justice Department and White House lawyer during the George W. Bush administration.

Meanwhile, a series of terrorist attacks in which gunmen used encrypted phones has convinced some lawmakers it is time to bring tech companies to heel. Apple’s absolutist position on encryption earned it bipartisan scorn at a Senate Judiciary Committee hearing in December. “This time next year, if we haven’t found a way that you can live with, we will impose our will on you,” said Judiciary Chairman Lindsey Graham (R-S.C.), a close Trump ally.

And Graham isn’t leaving things there. “Barr has called me and said he wants to have lunch,” he told POLITICO. “We’ve got to do something.”

A key difference between the current encryption fight and the one that followed San Bernardino highlights Barr’s political gamesmanship, according to experts on both sides of the issue.

In 2016, the FBI wanted Apple to write custom software to unlock the San Bernardino phone. Apple could have complied, but it refused, arguing that doing so would undermine its users’ security and privacy. The government took Apple to court, though prosecutors withdrew their demand after a third party sold the FBI a tool to unlock the device.

In the Pensacola case, the FBI already owns forensic tools designed to unlock the shooter’s phones. But if those tools can’t break into the phones — perhaps because the devices are damaged or misconfigured — then the bureau faces a quandary: Apple wouldn’t be able to break into the phones either, because of changes it has made to its mobile operating system.

“This is, in a sense, a fight about the fact that they can’t [help],” said Julian Sanchez, a senior fellow at the Cato Institute focused on technology and civil liberties. The Pensacola case “is being disingenuously framed as ‘Apple isn’t doing something they could,’” Sanchez said, “when ultimately the point is to lobby Congress because the FBI would like legislation requiring companies to create backdoors.”

The government regularly asks Apple for help accessing phone data and clearly chose to highlight the Pensacola case for a reason, said former NSA attorney Susan Hennessey. “Since it’s unlikely the government will actually get assistance in this case, I think a good guess is that this is about generating public awareness.”

Barr’s effort “seems more cynical” than Comey’s did, said Johns Hopkins University computer science professor Matthew Green. “It seems more political.”

The White House declined to comment on its encryption strategy. Apple also declined to comment. DOJ did not provide a comment. The FBI told POLITICO that its request for help was based on the “consensus” of its technical experts.

Obama’s aides didn’t openly back law enforcement’s demands for backdoors, and his White House quietly scrapped encryption proposals to avoid a backlash. In contrast, Hennessey said, the Trump White House has ceded the initiative to law enforcement agencies by not offering those agencies any guidance beyond Trump’s tweets.

The result is an environment that may be more worrisome to Silicon Valley.

Tech companies felt "more comfortable in their position and less under pressure" during the Obama era, said a former FBI official who requested anonymity to discuss the 2016 confrontation. Now, Trump and Barr's less-deliberative approach is making CEOs nervous.

During the 2016 presidential campaign, Trump urged supporters to boycott Apple until it helped unlock the San Bernardino iPhone. He later vowed to stop using his iPhone if Apple didn't back down, although he uses the device today.

Trump weighed in again last week after Barr's press conference. The president slammed Apple for "refus[ing] to unlock phones used by killers, drug dealers and other violent criminal elements" and declared, "They will have to step up to the plate and help our great Country, NOW!"

Apple "could have given us" access to the Pensacola phones, Trump told CNBC on Wednesday, shortly after dining with Cook and other tech leaders in Davos. The president said he understood concerns about backdoors but added, "If you're dealing with drug lords, if you're dealing with terrorists, and if you're dealing with murderers, I don't care. We have to find out what's going on."

The former FBI official noted: "There's a very different tone coming from the White House now than there was before."

While Obama urged Silicon Valley to compromise with law enforcement, he never echoed Comey's stark language ("encryption threatens to lead all of us to a very dark place") the way Trump has backed Barr. "Comey was very, very hard on Apple the last time," said Cindy Cohn, the executive director of the Electronic Frontier Foundation, a civil-liberties group. "Obama just wasn't personally so critical."

But given Trump's mercurial nature, some experts questioned the impact of his words.

"The president's tweets are stronger than any statement from President Obama on the topic," said Baker, now of counsel at Steptoe & Johnson. "How firmly the president will hold to those views, though, is unknowable right now."

For now, it is clear Barr is leading the charge. As a former telecommunications lawyer who led DOJ during the technological disruptions of the early 1990s, Barr is familiar with law enforcement's need to intercept communications. People close to him recently told The Wall Street Journal that he is "surprised" encryption still stymies law enforcement and is "disturbed … by what he sees as tech companies' ability to essentially defy court orders."

To break the impasse, Barr can consult with investigators and prosecutors who struggle with encryption every day, as well as former law enforcement officials who dealt with the San Bernardino case.

"He's trying to learn from what went well and what didn't in that fight," said Baker.

One lesson from San Bernardino is that it helps to play to people's emotions. The Obama administration built its case around a terrorist attack, while Trump officials' opening salvo last year was a summit about how encryption made it harder to rescue kidnapped and exploited children.

“The American public will never side with the terrorist or child molester [by] saying they have rights worthy of protection, and DOJ knows this,” said Andre Mcgregor, a former FBI cyber agent.

While Barr is a powerful voice inside the administration, any victory will require convincing the president to overrule other advisers who urge restraint.

And despite the president’s attacks on Apple, the administration is “divided” on encryption, according to a former Trump transition official familiar with the administration’s thinking.

“The hardcore national security types are adamant on encryption and the rest of the administration is not so sure,” this person said, adding that Treasury Secretary Steven Mnuchin and National Economic Council Director Larry Kudlow are worried that a backdoor mandate would undermine U.S. tech firms’ global competitiveness. (Asked for comment, a Treasury spokesperson pointed POLITICO to a CNBC interview in which Mnuchin called encryption “a complicated issue” and declined to say what solution he favored. The economic council declined to comment.)

Recently departed senior administration officials think the White House will “fold” on encryption, according to the former transition official. This person noted that Cook is close to members of the Trump family.

And while Trump officials clearly sense an opportunity, some aspects of the current political climate may work in Apple’s favor compared with 2016, despite the anti-tech backlash brewing in D.C.

For one thing, Hennessey said, “there is dramatically less public confidence in the Justice Department’s institutional integrity,” following years of bipartisan criticism of DOJ over issues such as immigration, its degree of political independence from Trump and its probes into Russian election tampering. That “makes seeking a solution more challenging,” she said.

Pro-encryption activists also argue that their message is gaining increasing acceptance. “The fact that you cannot build a door … that can only be used by good guys and cannot be used by bad guys is getting more and more obvious,” the Electronic Frontier Foundation’s Cohn said.

On the other hand, Congress may be more eager now to pass encryption-piercing legislation.

Lawmakers “are already mostly persuaded” to act, said Matt Tait, a cyber fellow at the University of Texas at Austin who testified at the December hearing.

DOJ’s top national security official recently said he had “never seen” the political climate “so conducive to passing some kind of encryption legislation … as it is today.”

But it remains unclear how many lawmakers who don’t sit on the law enforcement–friendly Judiciary panel will back Graham. Some, like Sen. Ron Wyden (D-Ore.), are pushing strongly in the other direction. Most members of Congress know little about encryption, and some on the Hill see Barr’s Pensacola push as a stunt.

Investigators already have plenty of information about the gunman, according to a House Democratic aide who participated in a recent briefing with DOJ officials.

“It did not strike me that their need to get into the cell phone was based on any investigative need,” the aide told POLITICO. “They were able to tell us that they knew all of the affiliations of the shooter. They had scrubbed his social media.”

Officials raised the issue of accessing the iPhones “almost as an afterthought,” the aide said. “Their need to get into these two particular devices strikes me [as] more a matter of politics … than it is actually a legitimate investigative need.”

The administration faces equally dubious odds of using Pensacola as a test case in court, because Apple lacks the ability to help. “I’d argue it is downright sanctionable to even attempt [to litigate] this,” said Weaver, of the University of California, Berkeley. “It would be like saying: ‘Hey court, compel this person to fly through the air without an airplane.’ Just the ask is ridiculous.”

Both supporters and opponents of restricting encryption agreed it was nearly impossible to predict how a fight that dates back to the 1990s would continue to morph in the Trump era.

People in the tech community hope the issue blows over once more, even as they prepare for another prolonged fight. Current and former law enforcement officials, meanwhile, think they may have finally found their moment.

“I don’t think anyone can say how these issues are likely to be resolved, either in terms of court rulings or legislation,” said Hennessey. “But this is just not a tenable situation over the long term. You can’t kick the can down the road forever.”