Apple bites back to keep the feds away

February 29, 2016

Last week Apple filed a motion to vacate a US magistrate judge's order to force the iPhone® geeks to work with the FBI to write new software to defeat its own security protocols to open the San Bernardino terrorist's work phone. The latest legal brief states that several of Apple's constitutional rights are being threatened.

"Can the government compel Apple to write software we believe would make 100s of millions of customers vulnerable around the world including the US and also trample on civil liberties that are the basic foundation of our what our country is made on," Time Cook, Apple CEO told David Muir of ABC News.

New Pew Research polling found that 51 percent of Americans' believe Apple should unlock the terrorist's work phone while 38 percent dissented.

"This is not about a poll this is about the future and what I've seen as people understand what is at stake here, we have increasing support," Cook explained. "If the court can ask us to write this piece of software, think about what else they can ask us to write. Maybe it's an operating system for surveillance; maybe it's the ability for law enforcement to turn on a camera. I mean I don't know where this stops."

The leader of the iPhone® giant firmly believes this case should not be heard in the court of public opinion, but rather in the US Congress where lawmakers can fully vet the action in front of their constituents.

"If there should be a law that compels us to do it, it should be passed out in the open and the people of America should get a voice in that. The right place for that debate to occur is in Congress."

Democrats agree that this probably won't be resolved in the courtroom.

"This case has much broader policy implications, which is why ultimately the court decision won't decide this issue," Rep. Adam Schiff (D-CA), House Intelligence Committee, told CNN. "Ultimately, it's going to fall on us in Congress to try to draw the line, in terms of what the technology sector must or must not do."

"The parties have to find common ground, and Congress needs to write it into law," Rep. Patrick Meehan (R-PA) wrote in The Hill newspaper.

However, Cook says tech firms always have to consider that hackers are always probing their devices to find backdoors. Something smart phone users should also consider is their hand-held

devices contain personal information about their daily lives. Standing firm on his beliefs, Cook says, the company will not bow to critics who argue this was a terrorist attack and that changes the rules. Giving the government free reign into smart phones could also unlock the government's power to turn on cameras or microphones remotely unbeknownst to the owner. It is this power that Cook finds offensive to the Constitution.

"It would also set a precedent that I believe many people in American would be offended by so when you think about those that are known compared to something that might be there I believe we are making the right choice."

The government's argument rests on the premise "just this once and just this phone" when in fact they know that statement is not true, Cook says. According to state and local representatives, they would seek relief from this ruling because they have hundreds of devices they would like opened, the majority of these have nothing to do with terrorism.

"This case is an awful case - there is no worse case than this, but there may be a judge in a different district that feels that this case should apply to a diverse case, there may be one in the next state over that should apply in a tax case another state over it should apply in a robbery you begin to say this is not how this should happen," Cook contends.

Also backing up Apple's position is Lowell McAdam, Chief Executive of Verizon Communications which sells iPhones®. They support "the availability of strong encryption with no backdoors. The case with Apple presents unique issues that should be addressed by Congress, not on an ad hoc basis."

Another point to remember is the government has had some of the worst security breeches in the world, including the Office of Personnel Management, which lost personnel data of 22 million current employees of the federal government. The bad guys will find it too. Once the bad guys know that additional info can be hacked they would stop at nothing to get that software and exploit it to harm the US.

But what are the chances that a favorable court ruling would open the door to law enforcement cases asking for relief? (The CIA/DOJ already spying on phones story by this reporter.)

"I do think that it is potentially, whatever the Judge's decision is in California and I'm sure it will be appealed no matter how it ends up, (and) will be instructive for other courts and there may well be other cases that involve the same kind of phone and same operating system," James Comey FBI Director said. On top of that, the director is on the record stating the government does not believe there is critical information on the phone in question that belongs to the county of San Bernardino. Furthermore, the FBI admits it made an error in triggering the security mechanisms of the phone prior to searching the cloud storage for the information.

"Apple is challenging the judge's order, and the standoff could lead to a new legal precedent on investigators' ability to compel private companies to help them penetrate the security around their devices and software. A federal judge in New York is weighing similar issues in a drug investigation; and around the country, the Justice Department is seeking a dozen other court orders compelling Apple to help them open iPhones®," the FBI director said in WSJ. "This is the hardest question I've seen in government, but it's going to require negotiation and

discussion," Mr. Comey said, but also admitted precedent could be set. "I love encryption, I love privacy,'' Director Comey repeatedly said.

One such case was Lavabit, an encrypted email service that shut its doors rather than provide the government a backdoor key to retrieve customer information. It has also prompted other companies to open doors outside the US, offering more secure, encrypted devices like Blackphone®.

Unfortunately, Congress appears to employ terrorism to unite American fear rather than legislate a permanent solution for the ever-changing electronic revolution. In the meantime, lawmakers and bureaucrats will ignore the use of ex parte hearings and in camera reviews behind closed courtrooms as the preferred method to escape public scrutiny for continued civil liberty violations.

Plus, Apple contends the writ would force it to "use the location of suspects, or secretly use the iPhone's microphone and camera to record sound and video. And if it succeeds here against Apple, there is no reason why the government could not deploy its new authority to compel other innocent and unrelated third-parties to do its bidding in the name of law enforcement. For example, under the same legal theories advocated by the government here, the government could argue that it should be permitted to force citizens to do all manner of things 'necessary' to assist it in enforcing the laws, like compelling a pharmaceutical company against its will to produce drugs needed to carry out a lethal injection in furtherance of a lawfully issued death warrant, or requiring a journalist to plant a false story in order to help lure out a fugitive, or forcing a software company to insert malicious code in its auto-update process that makes it easier for the government to conduct court-ordered surveillance. Indeed, under the government's formulation, any party whose assistance is deemed "necessary" falls within the ambit of the All Writs Act and can be compelled to do anything the government needs to effectuate a lawful court order. While these sweeping powers might be nice to have from the government's perspective, they simply are not authorized by law and would violate the Constitution."

But, it's also important to point out that the smart phone giant has censored apps, submitted to security audits and has moved local user data to Chinese state-owned servers. Clearly Apple wants to do business with China's 1.3 billion people who are not protected by the same Bill of Rights as US consumers.

Civil libertarians have warned the surveillance state is one legal case away. "Rather, it's a fight over the future of high-tech surveillance, the trust infrastructure undergirding the global software ecosystem, and how far technology companies and software developers can be conscripted as unwilling suppliers of hacking tools for governments. It's also the public face of a conflict that will undoubtedly be continued in secret—and is likely already well underway." There are four main components Americans should consider before throwing their support behind the US government, according to Julian Sanchez, is a senior fellow at the Cato Institute.

"This offers the government a way to make tech companies help with investigations; this public fight could affect private orders from the government; the consequences of a precedent permitting this sort of coding conscription are likely to be enormous in scope; and most ominously, the effects of a win for the FBI in this case almost certainly won't be limited to smartphones. These, then, are the high stakes of Apple's resistance to the FBI's order: not

whether the federal government can read one dead terrorism suspect's phone, but whether technology companies can be conscripted to undermine global trust in our computing devices. That's a staggeringly high price to pay for any investigation," Sanchez explained.

It boggles the mind to think that US courts would be willing to issue such sweeping judicial powers to the FBI based on an FBI screw-up in handling the smartphone's security features and the admission by Comey that the phone does not contain any critical information.

In breaking news, a federal judge in New York, has denied the government's efforts to force Apple to assist law enforcement officers' skirt an iPhone® passcode belonging to a person who plead guilty to drug charges. The ruling could affect an Apple case in California where the FBI is requesting the company assist law enforcement circumvent the passcode on a work 5c iPhone® used by the terrorist in the San Bernardino shootings.

US Magistrate Judge James Orenstein rejected federal prosecutors' claim that a 1789 law gives the government the right to obtain a court order that would bypass the passcode-lock on a phone. "Nothing in the government's arguments suggests any principled limit on how far a court may go in requiring a person or company to violate the most deeply-rooted values to provide assistance to the government the court deems necessary," Orenstein wrote.