Will FBI Take a Bite Out of Apple? Former CIA Agent on Showdown Between Apple & U.S. Government

February 25, 2016

As the government continues to take a bite out of Apple, Apple CEO Tim Cook says the FBI's request to unlock the iPhone of one of the San Bernardino shooters is the "software equivalent of cancer." In an interview on ABC, he explained why the tech giant is resisting a court order to help unlock the phone. TheFBI says Apple is overstating the security risk to its devices, and argues the litigation is limited. "It won't be unique to this one phone. It would be something that the government can use against any phone. And even if you think that it's OK for the government to be able to break the encryption of anybody's phone … what backdoor is accessible to the U.S. government would also be accessible to whatever is the American enemy du jour," says our guest Barry Eisler, who has written about government surveillance in fictional form. He is also a former CIA agent. Eisler is the author of several books, most recently, "The God's Eye View."

TRANSCRIPT

This is a rush transcript. Copy may not be in its final form.

NERMEEN SHAIKH: We turn now to the ongoing dispute over privacy and encryption between the FBI and the computer giant Apple. In an interview last night on ABC, Apple CEO Tim Cook explained why his company is resisting a court order to help unlock the iPhone of one of the San Bernardino attackers. In December, Syed Farook—Syed Rizwan Farook and his wife killed 14 people and injured 22 others. The two attackers were killed in a shootout with police. Cook said what the U.S. government was asking Apple to do was the, quote, "software equivalent of cancer."

TIM COOK: This case is not about one phone. This case is about the future. What is at stake here is: Can the government compel Apple to write software that we believe would make hundreds of millions of customers vulnerable around the world, including in the U.S.? The only way we know would be to write a piece of software that we view as sort of the software equivalent of cancer. We think it's bad news to write. We would never write it. We have never written it. And that is what is at stake here.

AMY GOODMAN: The FBI says Apple is overstating the security risk to its devices, and argues the litigation is limited. In an open letter earlier this week, FBI Director James Comey wrote, quote, "The particular legal issue is actually quite narrow. ... We don't want to break anyone's encryption or set a master key loose on the land," he said. Apple phone systems have a function that automatically erases the access key and renders the phone permanently inaccessible after 10 failed attempts.

To talk more about the case, we're joined by Barry Eisler, who has written about government surveillance—in fictional form. But he's also a former CIA agent. Eisler is the author of a number of books, most recently, *The God's Eye View*.

It's great to have you with us.

BARRY EISLER: Thank you, Amy. Good to be here.

AMY GOODMAN: So, let's talk about what the government is doing and the pushback of Apple.

BARRY EISLER: Yeah, I like Tim Cook's metaphor. It's nice to see someone hitting back linguistically this way. You would expect the FBI to say what it's saying: It's only about one phone. This is the kind of thing the government always says. And I'm reminded of the time the CIA acknowledged that it had made two torture tapes. Fifteen months later, it acknowledged that it was in fact 92. In this case, the government said this is only going to be about one phone, and it took them only a day to say, "Did we say one phone? Actually, we're talking about 12." If you talk to any encryption or security expert anywhere, they'll all tell you that what the FBI is asking for is impossible. You can't create a backdoor for one phone without making all phones vulnerable. So that's one important issue here.

But there's another one that I think is not adequately understood. As Julian Sanchez, a guy I follow pretty closely because he knows a lot about these things, works with the Cato Institute, put it, this just isn't about encryption, it's about conscription. And I wish people would understand this a little bit better. It's unprecedented for the government to be telling a private company what products it can create and what features it has to include in those products. As Tim Cook pointed out, where does this stop? What if the government said, "We want to have a feature on the iPhone that enables the FBI to turn on the iPhone camera, to turn on the iPhone microphone, anytime we want? Would that also be OK?" So, I hope this isn't going to happen. It's sort of odd have to be championing the world's richest corporation in its fight with the government.

AMY GOODMAN: I mean, they're asking the Apple to write a program, which would then create a backdoor.

BARRY EISLER: Exactly. And it won't be unique to this one phone. It would be something that the government could use against any phone. And even if you think that the U.S. government—it's OK for the government to be able to break the encryption of anybody's phone, even if you trust the U.S. government and think the U.S. government has never lied anyone, never abused its powers, even if you believe anything like that, what backdoor is accessible to the U.S. government would also be accessible to whatever is the American enemy *du jour*—could be the Chinese government, Russia, Iran, and, of course, not just to state actors, but also to

criminal groups and hackers. A vulnerability in a phone is not accessible to just one actor. It becomes vulnerable to everyone.

AMY GOODMAN: But he killed 14 people, he and his wife.

BARRY EISLER: Yeah.

AMY GOODMAN: And they just want access to see if there's other plans. I mean, who knows what would be?

BARRY EISLER: So this is another thing the government is typically good at. It tries to find the most attractive fact pattern it can to use as the thin edge of a wedge that it can then use in other less obvious fact patterns. And I see this again and again. People don't remember that well now, but José Padilla—I'm sure you guys remember—the so-called dirty bomber, I mean, José Padilla was accused of trying to create a radiological bomb and detonate it in Chicago, and a whole lot of people were going to die. And so, to keep us safe from that kind of thing, the government arrested him, held him on a Navy ship, offshored him—no due process, no charges, no trial, no access to a lawyer. It was unprecedented. But they were careful to choose what for them was an attractive fact pattern, before doing something so unprecedented. They picked a scary-looking guy and accused him of doing scary things. And people didn't protest the way they would have if they had chosen someone a little bit different.

So it's the same thing here. They're not doing this in the name of, I don't know, preventing someone from shoplifting or something like that. They've chosen a very attractive fact pattern so that they can say the talking points that you were just parroting, which is like, "Come on, this is just to keep us safe from the really scary people who want to kill us all in our beds," and who indeed did kill a lot of people in San Bernardino.

NERMEEN SHAIKH: So, to what extent do you think that accounts for public opinion? Because a recent Pew [Research] Center poll found that 51 percent of Americans think Apple should comply with the FBI and unlock the iPhone of one of the perpetrators of the attacks, and only 38 percent said that the FBI should not, and the rest had no opinion.

BARRY EISLER: Yeah, which is not actually—which is not a bad response to anyone who thinks that Apple is doing this as some sort of publicity stunt. I mean, for the moment, anyway, more people think that Apple should comply than think that it shouldn't. I think the fact that so many people, actually, that 38 percent, think it's a really bad idea for Apple to be forced to do this is, in part, a tribute to the educational value of the Snowden revelations and all the journalism that's been built on them, because I'm pretty sure—can't really conduct this experiment, but I'm pretty sure that if it hadn't been for Snowden's revelations, the public would be focusing entirely on the keep-us-safe-from-the-terrorists aspect of this whole thing, and not on the but-this-is-going-to-destroy-privacy aspect.

AMY GOODMAN: I mean, interestingly, Apple has made the iCloud available. It's not like they haven't done that. I mean, there have been many requests of these different phone manufacturers to get access to the iCloud.

BARRY EISLER: Right.

AMY GOODMAN: And, I mean, the government can't just get access to it; they have to get permission.

BARRY EISLER: Right.

AMY GOODMAN: So they're making a distinction between the actual physical phone—

BARRY EISLER: Right.

AMY GOODMAN: Apparently they turned off the iCloud at some point—

BARRY EISLER: Right.

AMY GOODMAN: —so it's what's remained on that phone since the point they turned it off.

BARRY EISLER: Right. So, the idea here is that some of your data is not accessible even by the company that created the product. It's on your local device, and no one else should have access to it but you. Apple has, in fact, complied with the government in the government's request to turn over data to which it has access. Maybe people might like that, they might not like it. My own feeling is, look, as long as it's pursuant to a warrant and it's not secret and it's out in the open, I can live with it. But the notion that now Apple is going to crack encryption that its users have come to rely on to keep their data private is—is an entirely new thing.

NERMEEN SHAIKH: Well, I want to turn to comments made by Bill Gates, the co-founder of Microsoft. He was asked about the ongoing dispute between Apple and the FBI, and said it was important to strike a balance between privacy and government access. Gates was speaking to Bloomberg.

BILL GATES: The extreme view that the government always gets everything, nobody supports that; having the government be blind, people don't support that. ... I do believe that—that with the right safeguards, there are cases where the government, on our behalf, like stopping terrorism, which could get worse in the future, that that is valuable, but striking that balance. Clearly, the government's taken information historically and used it in ways that we didn't expect, going all the way back, say, to the FBI under J. Edgar Hoover. So, I'm hoping now we can have the discussion. I do believe there are sets of safeguards where the government shouldn't have to be completely blind.

NERMEEN SHAIKH: That was Bill Gates speaking to Bloomberg News. Your response?

BARRY EISLER: It's interesting. He's so close to an epiphany. He talks about J. Edgar Hoover. Maybe he knows about COINTELPRO. He acknowledges that the government has abused powers that it's been given in the past. And so, you think he's going in a certain direction with this, and then he just comes up with this platitude, which is we have to strike a balance. Like who doesn't think that we shouldn't strike a balance? It's just meaningless. There's no one who would say, "I don't think we need a balance. I think it's just one or the other." So, I don't know. Maybe it's not a coincidence that Microsoft is a fading technology company and Apple is a premier one.

AMY GOODMAN: Microsoft has said that in the past, that 80 tech companies have cooperated—I mean, WikiLeaks has said that 80 tech companies in the past have cooperated with the NSA, the National Security Agency, including Microsoft.

BARRY EISLER: Yeah, so much of the—of Snowden's revelations were about this very thing. And the fact that the public knows about corporate cooperation with the government now is in part, I think, what has emboldened Apple to push back, because, again, if we didn't know about these things, I would expect that Apple would be quietly cooperating. There would be no cost to their doing so. But they realize now that there's a significant constituency among their customers that wants robust privacy features in Apple products, and to please those customers, Apple realizes that in this public battle with the FBI, it can't just roll over and serve the FBI; otherwise, it might turn into the next Microsoft.