McAfee: If FBI gets backdoor to people's phones, US society will collapse

22/04/2016

Law enforcement, drug trade, political fights and terrorism have gone online. The fight for information and access to the hidden data is raging on, both in the legal sphere, with authorities trying to tighten the grip on the digital flow, and international, with army-like hacker groups searching for the cracks in the cyber defense of nations. How far will this fight go? Who has the upper hand? And can battles in virtual reality claim real lives? We ask the cyber-expert extraordinaire – John McAfee is on Sophie&Co today.

Follow @SophieCo_RT

Sophie Shevarnadze: *John McAfee, cyber security expert extraordinaire, inventor, entrepreneur, creator of McAfee antivirus, welcome to the show, once again, it's really great to have you with us. So, John, the recent Apple-FBI battle over the unlocking of encrypted Iphone of the San-Bernardino shooter has ended when the FBI said it was able to access the phone's data with the help from the third party. Should the FBI have access to the information stored on that phone, the phone of a terrorist?*

John McAfee: It's not the matter of should they have it. I mean, I guess, if he's suspected in a crime, the question is not whether they should have access to it, it is whether they should require Apple to give them access in a manner that gives them access to all other telephones, and that's basically what the FBI was asking.

SS: *But that's all inter-related. Do you believe the FBI did in fact get access to the phone, or did it just say it did to save face?*

JM: Oh yes, absolutely, they did get acess, it's no question - they have the ability to get the access all along. The way they got access was through a device built by an Israeli company called "Cellebrite". They had a contract with that company dating back to 2013 and it purchased thousands of these devices, so, they had the capacity all along. They just wanted to use this phone, since it was used in a terrorist act, to be a test-case to try and get the courts to force Apple to give them a backdoor.

SS: *So they had to involve a third party to actually hack into that Iphone, because you've said that the FBI doesn't have the capacity to carry out an Iphone hack, for instance, on its own. Why not? Why doesn't a powerful agency like that have the resources to make things done?*

JM: Well, I mean, they have the resources since they've purchased these devices, that's one way of saying they have it. I think the FBI is behind the Apple, they don't have the capacity anymore to keep up with the changing technology. It's a very tired organisation that doesn't inspire creativity and innovation, and they need to follow other countries in expanding their hiring and structuring their security programs and their cybersecurity. They just haven't kept up.

SS: *So, Apple has been refusing to help the FBI to get inside the phone and they were saying it would actually compromise the security of all other devices. But, after the cracking the phone, however, the FBI was quick to say that the method they used won't work on more advanced Iphone models. So, one of the sides is definity bluffing, which one?*

JM: The FBI is bluffing. The devices they have will actually break into any iphone. It's a hardwired device. It's not a software key that you can just transmit over the internet and let everybody have it. no. It's a hardware device. They have to buy the device, they have to have the device present and they have to put the phone into that device. So, no, the FBI is bluffing. They have the capacity, using that same company - Cellebrite - to get access to an Iphone system.

SS: *How can Apple actually counter all of that? Can it counter all of that, all this new hacking?*

JM: Here's the truth of hacking and security. No matter how secure you want to make your system, someone will always find a way to break in. It's been that way with safes, it's been that way with door locks, it's been that way with bank vaults. There will always be a way. Nothing can be perfectly secure in life. This is just the way the world works, the least of all, software. It has to be a continual affair. You make something, you think it's perfect, someone finds a way to break in, you see how they break in, you fix that and make it stronger. And in the end, we end up with stronger products and more perfect security.

SS: *Wall St. Journal says Apple has been helping the FBI break into Iphones of criminals since 2008, but changed its policies after Snowden's revelations. So, Apple didn't really care much about user privacy before that, right?*

JM: Well, no, I disagree with that. I'm gonna take Tim Cook's and Apple's side in this. Apple has been helping and I have no problem with that. You only get access to an individual phone, you get a court order, Apple should help. But the FBI didn't ask for that. It asked for a universal key that will allow it to get into any Iphone. It's a different thing and it's the first time the FBI has asked for that. I'll be very surprised if Apple had not cooperated with the FBI, even after the Snowden's revelations. That's one thing. Sure, you have a court order, you have a phone you want to break in - we'll help you break into this phone; but the FBI specifically said "We want a Master Key". That's what they asked for.

SS: *Would you say FBI lost eventually, because Apple didn't hand over the universal key to FBI?*

JM: Well, no. Actually, the FBI has not lost because now they have a new core challenge from the state of NY over an Iphone that belonged to a drug dealer. So they're now trying a new challenge using the same exact arguments. So, no, this may go on for quite a while, the FBI continuing to push and then backing off and then continuing to push, and then backing off…

SS: *And then eventually using third parties to hack into those devices.*

JM: Yes. So this is going to be a constant. But Apple can never give in, they simply can't. We all lose if the people who built the privacy systems give up, give up on privacy, give up on their product and give up on us, so it can't happen, not in my world.

SS: *So here's a funny detail: director of the FBI has admitted to be covering his laptop camera with a tape to guard his privacy. So the same person who wants a backdoor into private data is worried about being spied on by someone. How does it even work? And, if he does it, should we all be doing that, should we all be covering or laptop cameras with a tape?*

JM: No, no. All it shows is the lack of sophistication within the FBI, because there are a lot of products available… I make a product through my company Future Tense Central called D-vasive that you can download and lock it by clicking a button: if you want to lock the camera, lock the camera, lock the microphone, lock whatever you want. That's available. The fact that the director of the FBI uses tape - tape! - instead of using the more sophisticated software that the rest of us use - doesn't that scare you? It scares me.

SS: *Yeah, but some would argue that this really conventional techniques like using tape or I don't know, typewriters, is the only sure way not to be hacked in, because once you have a program protecting, there's an anti-program that hack into that program that protects you.*

JM: Yeah, but what does the tape do? It doesn't prevent software from getting hacked into…

S*S:* *You can't hack into a tape.*

JM: No, no. The tape only covers the camera, meaning that the camera cannot take a picture of you. It doesn't cover the microphone, it doesn't cover the… you're still on the internet. So, no, the tape does nothing other than lock the camera from taking a picture. That's what I'm saying. You can still get software in. It's a piece of tape that... you have on the laptop and on your phones, you have a tiny little circle which is the camera lens. People put tape over that, so that the camera cannot see them. Okay, so you're being protected from being watched, but you're not being protected from being listened to and you're not being protected from software getting into your system and stealing your data. It's a very unsophisticated approach.

SS: *So why are they so unsophisticated? Because there's no other reason behind using things like tape other than being unsophisticated? There's no other thoughts behind that, right?*

JM: No, there's no other reason at all. That's what we used to do before we got software to do it for us. No, they're unsophisticated because they have not kept up with changing technology, obviously.

SS: *To that point?*

JM: Yes, to that point, obviously, as he admitted to doing it. He admitted to doing it. So tape doesn't prevent you from getting hacked. It does not prevent you from getting your data taken, it does not prevent you from being listened to. All it does is prevent the camera from seeing you. So, no, if he believes that it actually prevents hacking them, we all need to just go home, because we're lost.

SS: *How can the FBI not be on top of all of these things, seriously? I find it hard to believe.*

JM: Isn't that the question? I mean, seriously, is that not the question? I mean, maybe they are and they're trying to delude us for some bizarre reason because when they came to Apple and said "we can't get into this phone", they could. They had the device from Cellebrite to do it. So, this is an utter and complete nonsense. It's nonsense. But, I actually believe that the director is using tape, because it sounded legitimate, it sounded like he was being sincere. What is shows us, he doesn't understand cyber science at all, which means that maybe the whole FBI doesn't not understand it - because, really, if you're the head of the FBI, and cyber science is 90% of your work and you don't understand it, we have a problem either way you look at it; no matter how you approach this situation, it's tragic and it bodes ill for me and you and all Americans. Please, it's so obvious!

SS: *So, we've established that everything can be hacked. Is there any phone that's truly safe and spy-proof or users? There's no way to avoid spyware?*

JM: Absolutely. It's a phone that doesn't have a computer in it. They're called "dumb phones", and you can call anybody you want and even send text messages and they cannot be hacked because there's nothing in them to hack. But beyond that, if you have a smartphone, when you have a computer and you have software, someone will always figure out a way.

SS: *Encrypted Telegram messenger faced criticism for being used by terrorists. You know, we have a moral dilemma here; now, WhatsApp has joined the encryption club. Do you expect a law enforcement crackdown on all these encrypted messengers, privacy-guarding business?*

JM: Yes, of course. Why should law enforcement have the right to listen into my private conversation. I mean, if I want to go out into the woods and whisper something to my wife, I should have the right to do that. I have the right to privacy.

SS: *Does a terrorist have a right to privacy?*

JM: How do you know they're a terrorist? I mean, a "suspected" person is not a guilty person. Until you're proven guilty, you have all the rights that everybody else has. This is America. We have a Constitution. I am sorry, and I am not a terrorist, and neither are you to my knowledge, and just because there are terrorists, should you give up your right to privacy? Absolutely not! Do you realize what madness that would bring, what chaos? Our society would become unglued. We can't do that.

SS: *You know, the most damaging cyber-attack on record, the Panama Paper leak. It affected major law firm that's working with the heads of states, politicians, celebrities. Now you called the Panama Papers a "smear" campaign orchestrated by the U.S. government. Do you mean to say the government's hackers are behind it? I mean, what evidence is there that the U.S. government has orchestrated all of this?*

JM: I'll give you the evidence. There were 14000 companies in their, fourteen thousand! Not one American?

SS: *Americans tend to have their offshores in Bahamas rather than Panama. That's not a proof.*

JM: That's not true. That's absolutely not true. I mean, I know lots of Americans who have Panamanian offshore accounts, many of them. They do it because they want their money protected, they don't trust the American banking systems, and then don't trust American privacy laws, so they do that. No, that's utter nonsense. I mean, the Icelandic people were using it!

SS: S*o, you're really saying that the American government orchestrated this whole Panama leak?*

?)Well, I'm saying that they certainly had a hand in it, yes.

SS: *But, what would be the reason? Why would they do that?*

JM: Oh, half of it has already been expressed: using these papers, America got to smear the government's enemies. Who was released? Iran, Pakistan, I don't know why… Oh, I know why Iceland was in there, because they had made some enemies in the face of some powerful banks.

SS: *No, no. I mean, they had Cameron's family involved, they had Azerbaijani family involved. They are all American allies.*

JM: But no, that was by very very slight implication, very slight implication. Directly, the PM of Iceland and look at all of the links that they tried to make to Syrian leaders and Palestinian leaders about drug money and weapons, all of these other things, terrorism. And not one word about America? Why would they do that? Number one: it lets us smear our enemies, and then they had smeared some others to make it look legitimate, and then, it gets to tell the American people who do have accounts with Mossack Fonseca that "we know that you're in there". And suddenly, powerful American people have the government holding something over their head. You know how this works, you know how this works. This is politics in the world at large, not just in America. It's sad, it's tragic, it's heinous, but it's real. It is what happens. Please, governments become corrupt always. Power inevitably corrupts, and absolute power corrupts absolutely. Please, this is the truth of life since the beginning of the human race. And, so, our government… can you say our government is not powerful? If it is powerful, there's corruption somewhere in it, to a very high degree; and so to imagine that the U.S. government would never do something like that? Look, at what our government has done, these guys have been spying on us among other things, by an agency whose charter is to spy on foreign nations.

SS: *On the other hand, Chinese hackers have allegedly breached U.S. government personnel records. Why can't even the U.S. government actually protect its own data?*

JM: Isn't that the question? Let's get back to why does the head of the FBI put a piece of tape over his camera lens, thinking that it's going to protect him? It is because we are very far behind. Obviously, the government says "no, no, we are very advanced in cyber warfare and cyber technology". If that's the case, why did you allow the

Chinese to walk off with 21 mn records from the Office of Personnel Management? Why did you let the Iranian government almost open sluice gates on a power dam in New York? Why did you let Homeland Security get hacked? The Pentagon? The FBI? Two fifteen-year old boys hacked into the FBI database and walked off with all the personal information of their undercover agents. Good gosh, if we know what we're doing, why is this happening to us? The only answer is: we don't know what we're doing! We don't know what we're doing. It is obvious to anybody who wants to take a look.

SS: *Alright, John, I want to talk a bit about cyber war against terrorism. I mean, you've said that America is stuck in thinking that eavesdropping will be effective against terrorism. If that's the case, then why there's this monster of a surveillance system in place?*

JM: Eavesdropping doesn't work, obviously. We've had one of the greatest eavesdropping organisations in the world. We're using all kinds of devices to listen in on people's conversations. Have we stopped a single terrorist attack? Not that I am aware of. And why, if we could stop one, why can't we stop others? I mean, it takes us by surprise every time, so, obviously, the eavesdropping technique is not working! They need another paradigm, they need to use a completely different technique. We are stuck in the 1930s, when we used to fight organized crime that rose out of our prohibition against drinking alcohol, we used to fight them by eavesdropping, and it worked so well. That was 70 years ago, please! The world has changed. Cyber Technology has changed the need and the methodology for cyberscience, and cybersecurity systems and cybersurveillance.

SS: *I read you said that there's another way to use raw data and patternized system to recognize terrorists out and predict their actions. But if the nation's security services are using it, maybe it's not that effective after all?*

JM: I mean, logic would say that it's extremely effective. We don't understand this issue in America. We still think that if we listen to the words that you say, that will tell us something. That is nonsense. With terrorist groups, the words that you say are always coded, that's another form of encryption: verbal encryption. They may be talking about basketball, in the end of the game, when score is done, and they are going to plan their next attack and you have no clue. But by watching the pattern of their calls - if this phone only does outgoing calls and never gets incoming calls; if prior to the attack there's one call made to ten people and from those ten people - ten more, and from those ten people - ten more - well that tells me something! That's a real life event that cannot be veiled by verbal encryption or by any kind of coding.

SS: *That's just good old fashioned spying, John. Tell me something: you've predicted a cyber war more devastating than a nuclear war. What kind of a big attack on the Internet is really possible? And honestly, I mean, blacking out websites doesn't sound that dangerous to me, compared with losing real lives; why should we be afraid of cyber-terrorism? Is it capable of more than internet disruptions?*

JM: Yes. Let's look at what's possible of being hacked. Any computer can be hacked. The older the computer, the easier it is to hack that computer. And what do computers do? They don't just access the Internet and do our taxes - they control steel mills and food-processing plants, and virtually, everything in life, including our cars now. Last year, a car was hacked into, by two hackers, hundreds of miles away and control was taken away from the driver. It was written up in Wire magazine. But let's assume there's something far more important than automobiles. Even airplanes can be hacked. What about power plants? In America, our power grid is approaching 50 years old, fifty! And our computers - 20 to 25 years old, way before cybersecurity was even considered as an issue. So, what if someone said:, instead of hacking your cell phone and stealing a credit card, I'm going to hack a power company and move all the power around until it blows out all the power stations? I think that's a serious problem. What if it blew out everyone? We'd have no power! Without power, we can't repair them, we have power tools. Without power we cannot process food, because all food processing is automated and controlled by computers. Without food, we die. I mean, okay. Mr. Pry, who was head of the Congressional Committee on EMP, which is Electro-Magnetic Pulse, and James Woolsey, the ex-head of the CIA presented the paper to Congress last year, insisting that if we'd lost our power grid, 90% of all Americans would perish within 24 months. I think that's optimistic. How can 10% of this live in a situation where there's no food and no fresh water? We're not used to going out and hunting and fishing for our food. Now sure, those 10% have a better chance of survival, but they're going to compete with a lot of hungry people, many of them armed. So, seriously, what could be worse? A nuclear war can't possibly impose that level of devastation, I don't care how bad that war might be.

SS: *Alright John, you sound pretty convincing. Well, anyways, thank you so much for this interview. We've been talking to John McAfee, legendary cybersecurity expert, inventor of McAfee security software, weighing in on questions of privacy and security in the digital age. That's it for this edition of Sophie&Co, I will see you next time.*