Written by **C. Mitchell Shaw** on March 2, 2016

Apple, FBI Testify Before Congress About Encryption

Representatives of both Apple and the FBI appeared before the House Judiciary Committee on Tuesday. Over a period of five and a half hours, the committee heard sworn testimony about the underlying issues in the case of the FBI attempting — via court order — to force Apple to create a backdoor for the iOS platform.

Testimony was heard from FBI Director James Comey (shown); Manhattan District Attorney Cyrus Vance, Jr.; Senior Vice President and General Counsel for Apple Bruce Sewell; and Worcester Polytechnic Institute Professor Susan Landau. The entire five-hour testimony was made available as a video on the committee's YouTube channel (testimony begins at 34:25).

Apple CEO Tim Cook has suggested that Congress, not the courts, should settle the issue of the legality of matters related to encryption. White House spokesman Josh Earnest has said that the courts should settle it, because "Sending complicated things to Congress is often not the surest way to get a quick answer." He added, "In fact, even asking some of the most basic questions of Congress sometimes does not ensure a quick answer."

With the tension between the executive and legislative branches duly noted, it needs to be pointed out that what is needed in this issue is not a "quick answer," but an *accurate* answer. And whether the courts or Congress are the best source of that answer is in doubt. As is too often the case, what is left out of the equation is the third option: Government has no business meddling in the private communications of private citizens. Encryption is the free market's natural response to the ubiquitous surveillance suffered by both the guilty and the innocent and should be left alone.

In his opening remarks, Comey admitted as much before shifting gears and condemning the very privacy he had just praised. Part of written his testimony reads:

> American citizens care deeply about privacy, and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.
>
> We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance — not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

> The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

After delivering his prepared statement, Comey was, as Engadget put it, "grilled pretty hard by the committee." As the tech-news site reported:

> While Comey continued to say that this is about a single device in a single case, New York DA Cyrus Vance was more forthcoming that law enforcement is being hindered by encryption and that he would like the ability to open the [encrypted devices] New York already has in its possession.

Engadget's description of Comey being "grilled pretty hard by the committee" is accurate, considering that Comey's testimony was *more than three hours long*. During that three hours, the most common answer given by the FBI director was one variation or another of "I don't know," or "I don't really understand how that works."

At one point, Congressman Darrel Issa (R-Calif.) — fed up with Comey's inability to answer simple questions about the technical tools and solutions the FBI had tried on its own before attempting to force Apple to create a backdoor — asked Comey, "How can you come before this committee — before a federal judge — and demand that someone else invent something if you can't answer the questions that your people have tried this?" Comey's answer was, again, a variation of "I don't really understand how that works." He replied, "I did not ask the questions you're asking me here today. I'm not sure I even fully understand the questions."

Vance's prepared statement included the following glaring admission which directly contradicts Comey's assertion that forcing Apple to help the FBI circumvent the encrypted iPhone used by one of the San Bernardino shooters would be a one-time deal:

> While the San Bernardino case is a federal case, it is important to recognize that 95 percent of all criminal prosecutions in this country are handled at the state and local level, and that Apple's switch to default device encryption in the fall of 2014 severely harms many of these prosecutions.
>
> And that is why I am here today as a representative of the thousands of local and state prosecutors around the country: Smartphone encryption has real-life consequences for public safety, for crime victims and their families, and for your constituents and mine. In the absence of a uniform policy, our nation will effectively delegate the crafting of national security and law enforcement policy to boardrooms in Silicon Valley. That is, important responsibilities of our government will be carried out by Apple, Google, and other technology companies, who will advance the best interests of their shareholders, not necessarily the best interests of our nation.

In case that was too ambiguous, Vance also told the committee, "Law enforcement agencies at all levels, as well as crime victims' advocates and other concerned community leaders, are watching this case with great interest." In other words, the surveillance hawks need this case to set the precedent so

that they can expand it to other cases.

Dr. Landau suggested that rather than ask private companies to collude with government agents by defeating their own security, the FBI might consider updating its own technical abilities. She also testified that forcing Apple to defeat the security measures protecting the encryption on the iPhone in the FBI's custody would have greater implications. She told the committee:

> The FBI has pitched this battle as one of security vs. privacy, but as a number of the members have already observed, it's really about security vs. security. We have a national security threat going on and we haven't solved the problem at all. What have smartphones got to do with it? Absolutely everything.
>
> Smartphones hold our photos and music, our notes and calendars, much of that information is sensitive — especially the photos. Smartphones are inreasingly [used as] wallets and they give us access to all sorts of accounts — bank accounts, DropBox and so on.
>
> Many people store proprietary business information on their smartphones, even their personal smartphones, even though they know they shouldn't.
>
> Now, NSA will tell you that stealing login credentials is the most effective way into a system. In fact, Rob Joyce of the Tailored Access Operations said so in a public talk a month ago. Here's where smartphones are extremely important: they are poised to become authenticators to a wide variety of systems and services. In fact, they are already being used that way in some high placed government agencies.
>
> Now, District Attorney Vance has said that large-scale data-breaches have nothing to do with smartphone encryption, but that's not true. Look at today's *New York Times* where there's a story about the attack on the Ukrainian power grid. How did it start? It started by the theft of login credentials of system operators. We've got to solve the login authentication problem and smartphones are actually our best way forward to do it. But not if it's easy to get into the data of the smartphones.

Apple's general counsel Bruce Sewell also argued that the implications of this case are more far-reaching than the case itself, telling the committee:

> The FBI has asked the court to order us to give them something we don't have — to create an operating system that does not exist. And the reason it doesn't exist is because it would be too dangerous. They are asking for a backdoor into the iPhone specifically to build a software tool that can break the encryption system which protects personal information on every iPhone. As we have told them, and as we have told the American public, building that software tool would not effect just one iPhone. It would weaken the security for all of them.
>
> In fact just last week Director Comey agreed — and I think we've heard the same here today — that the FBI would likely use this precedent for other cases involving other phones. We've heard from Distrct Attorney Vance who's also said that he absolutely plans to use this tool on over 175 phones that he has in his possession. We can all agree that this is not about access to one iPhone.

In the last few seconds of his remarks, Sewell made reference to U.S. Magistrate Judge James Orenstein's ruling the previous day in an separate case that "Granting the FBI's request [to force Apple to unlock an iPhone used by a suspected drug dealer] would thoroughly undermine fundamental principles of the Constitution." This was yet another point of embarrassment for Comey, who was

unaware of the ruling. In both that case (in New York) and this case, the FBI was attempting to apply the All Writs Act (from 1911) as a legal tool to compel Apple to create the software it needs to circumvent the software protecting the encryption of the iOS platform. Judge Orenstein's ruling called that use of the All Writs Act ridiculous and rejected the FBI's motion.

The good news is that the courts will likely follow that pattern moving forward, especially now that Congress is looking at the issue. The bad news is that Congress is looking at the issue. Concerned Americans need to pressure Congress to protect the rights of private citizens to keep their data and their communications private. But considering how often Congress has its own agenda, this really could go either way.

Photo: AP Images