Apple denies handing source code over to China

April 19 2016

Apple on Tuesday denied providing Chinese authorities with special access to its devices, as the iPhone maker defended its position on encryption and cooperation with US law enforcement.

The company's general counsel Bruce Sewell was appearing at a US congressional hearing on encryption's impact on law enforcement, as the high-tech giant battles the government over whether it should be compelled to help authorities in criminal cases.

Sewell said he wanted to set the record straight on China in light of reports cited by officials at the hearing that the company had turned over its software instructions or "source code"—which could be used to break encryption—to Beijing.

"We have not provided source code to the Chinese government," he told lawmakers.

"We have been asked by the Chinese government. We refused," he said, adding that this had happened "within the past two years."

Encryption debate renewed

The hearing was called to discuss how strong encryption is hampering law enforcement and how technology firms should respond to legitimate law enforcement requests to break encryption.

Lawmakers at the House Energy and Commerce committee said they hoped the discussion would help both sides in the debate find common ground, so that privacy can be protected while enabling law enforcement to get data its needs for criminal probes.

"I can't believe this problem is intractable," said Representative Diana DeGette. "What I want to hear... is about possible solutions going forward."

While law enforcement officials and Apple both expressed a willingness to talk, the comments appeared to show little common ground in a debate which has been raging for weeks.

The encryption issue hit a boiling point earlier this year when Apple refused to help the FBI weaken the operating system of an iPhone used by one of the shooters in last year's San Bernardino killing spree.

The government eventually withdrew the request, saying it had been able to get into the phone with help from an outside party, but similar cases are pending in the courts.

Sewell defended the company's toughened encryption for its iPhones, which can sometimes make data unreadable to authorities, even with a warrant.

"The best way we, and the technology industry, know how to protect your information is through the use of strong encryption," he said.

"Encryption today is the backbone of our cybersecurity infrastructure and provides the very best defense we have against increasingly hostile attacks."

An FBI official however repeated concerns that unbreakable encryption

may help criminals and terrorists evade detection.

"We have seen case after case—from homicides and kidnappings, to drug trafficking, financial fraud, trade secret theft, and child exploitation—where critical evidence came from smartphones, computers, and online communications," said FBI executive assistant director Amy Hess.

"Increasingly, some technologies are prohibiting law enforcement from having access to that critical evidence."

'In the dark'

Thomas Galati, chief of intelligence for the New York City police department, expressed frustration over the default encryption for smartphones.

He said that in the six-month period from October 2015 through March of this year, "we have been locked out of 67 Apple devices lawfully seized pursuant to the investigation of 44 violent crimes."

"In the past, a phone or wiretap—legally obtained through a judge—would alert the police to drop-off points, hideouts, and target locations," he said. "Now, we are literally in the dark. Criminals know it."

But Amit Yoran, president of the security firm RSA, said law enforcement is failing to use tools available to them.

"We live in a 'golden age' of surveillance, more so than in any other point in history," he told the panel.

"In just about everything we do, we leave an incredibly insightful digital

breadcrumb trail... Law enforcement has an overwhelming volume of information readily available to it, creating challenges to efficiently manage and fully leverage it."

Apple said in its most recent transparency report Monday that it received more than 30,000 data requests from law enforcement worldwide and provided some information in a majority of those cases.

© 2016 AFP