Encryption fears for law enforcement overblown: study

February 1 2016

Credit: Symantec

Encrypted communication is making law enforcement and counterterrorism investigations more difficult, but fears of "going dark" are overblown, a study said Monday.

The report by Harvard University's Berkman Center said that despite efforts to boost encryption in smartphone and online services, investigations still can gain access to data in many circumstances.

The study sought to evaluate claims by US law enforcement and intelligence officials that encryption is leading to a situation where they are unable to obtain data even with a legitimate warrant—a scenario described by some as "going dark."

"We question whether the 'going dark' metaphor accurately describes the state of affairs," the report said.

"Are we really headed to a future in which our ability to effectively surveil criminals and bad actors is impossible? We think not."

The researchers acknowledged that it has become increasingly difficult to get data from encrypted smartphones powered by software Apple or Google software.

But they also pointed out a distinction between data "at rest" on smart devices and in transmission.

"The distinction is important because an overwhelming percentage of Internet users communicate through web-based services, such as webmail, instant messages, and social networking websites that are not end-to-end encrypted," the report said.

"In the course of an investigation, government officials can intercept communications and seek access to stored communications held by these intermediaries by obtaining a warrant, court order, or subpoena, provided that the company is capable of producing the information sought," it added.

The encryption debate has heated up in the United States and other countries in light of concerns raised by FBI and National Security Agency officials who claim investigations are being hindered by encryption.

US presidential candidates and others have argued for solutions that could allow encrypted data to be delivered with an appropriate warrant.

But the Berkman report said that "short of a form of government intervention in technology that appears contemplated by no one outside of the most despotic regimes, communication channels resistant to surveillance will always exist."

It also noted that for national security, "we must consider whether providing access to encrypted communications to help prevent terrorism and investigate crime would also increase our vulnerability to cyber espionage and other threats."

The researchers said that despite the latest encryption efforts, many software systems are "fragmented" and that a lack of coordination will leave open some avenues for investigation.

The report said that with the number of connected devices on the rise, "this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access."

"The going dark metaphor suggests that communications are becoming steadily out of reach—an aperture is closing, and once closed we are blind," the report concluded.

"This does not capture the current state and trajectory of technological development."