Communications Daily

# Encryption Advocates Say DOJ Can Probe Without Weakening Security

Karl Herchenroeder

April 7, 2020

DOJ can investigate without weakening end-to-end encryption for messaging apps, representatives from BSA. The Software Alliance and Internet Society said in interviews, after Telegram told us the messaging app is under FBI investigation. Attorney General William Barr has repeatedly attacked end-to-end encryption (see 1910030058, 1910040035 and 2001220054), citing the dark web. The FBI is "obsessed" with breaking public encryption, said Cato Research Fellow Patrick Eddington. He cited bureau efforts since the 1990s and more recent interest in Facebook's WhatsApp.

It's unquestionable DOJ targeted WhatsApp, said BSA Senior Director-Policy Tommy Ross. He noted Barr's letter urging Facebook to forgo plans to deploy encryption across messaging services (see 1910030058). Telegram said that "as stated in the Privacy Policy, Telegram doesn't disclose private information of its users to third-parties. We suspect such investigations may be a result of us adhering to our privacy guidelines."

The SEC sued in October to block Telegram from launching a new blockchain network. The agency claimed the company was attempting to sell unregistered securities. Telegram "doubts" the FBI and SEC activity are related, a spokesperson emailed, saying the company believes the FBI probe predates the SEC's. The two agencies declined comment.

Major tech companies like Apple are acting in good faith and complying with law enforcement orders when necessary, said Ross. "They're not trying to play games." Encryption lets Apple provide better products, he said. The expert cited an FCC subgroup's report showing such security measures deter crime. In the six months after Apple introduced "activation lock" in 2013, iPhone theft declined by 38% in San Francisco and 19% in New York, said the Technological Advisory Council's subgroup. Police and industry need to explore solutions that protect both business and law enforcement interests, Ross said.

Data outside the encrypted stream can be used to capture criminals, said Internet Society Senior Director-Online Trust Jeff Wilbur. Allowing an encryption back door for police in one case exposes all users to the risk of a breach, he said. "It makes everything one click away from being exploited."

The FBI confirmed a "pending or prospective law enforcement proceeding" against Telegram in October, in a Freedom of Information Act response to the Cato Institute. Eddington is seeking documents on surveillance or investigation of Telegram and other tech companies to determine what data the agency is gathering.

Given the number of nefarious actors who allegedly use Telegram, the bureau could be conducting multiple probes that involve the company, Eddington said. Ross questioned whether Telegram is complying with legitimate law enforcement requests. There's a bright line between choosing not to comply with warrants and being unable to comply, Ross said, citing Apple's testimony on the latter (see 1912100039). He noted Apple regularly publishes transparency reports.

Telegram publishes information about private data disclosure, noted its spokesperson: The company hasn't published anything in this instance because it hasn't received a court order confirming a user is a terror suspect. The platform said it may disclose IP addresses and phone numbers to authorities if it receives such orders.

It isn't up to Telegram to decide whether a user is a criminal, Eddington said, calling the stance a "clumsy dodge." Police obtain warrants, and courts determine guilt, he said. "The question is whether Telegram has received law enforcement requests pursuant to criminal investigations."