TECHNEWSWORLD

Facebook Won't Let US, Australia, UK Get Toe in Backdoor

John P. Mello Jr.

December 11, 2019

Facebook on Monday rejected a request from the United States, the United Kingdom and Australia for a "backdoor" in its end-to-end encrypted messenger apps to help law enforcement agencies combat crime and terrorism.

"Cybersecurity experts have repeatedly proven that when you weaken any part of an encrypted system, you weaken it for everyone, everywhere," WhatsApp head Will Cathcart and Facebook Messenger head Stan Chudnovsky wrote in a letter to U.S. Atty. Gen. William Barr, Acting U.S. Homeland Security Sec. Chad Wolf, UK Home Office Sec. Priti Patel, and Australian Minister of Home Affairs Peter Dutton.

"The 'backdoor' access you are demanding for law enforcement would be a gift to criminals, hackers and repressive regimes, creating a way for them to enter our systems and leaving every person on our platforms more vulnerable to real-life harm," the Facebook executives maintained.

"It is simply impossible to create such a backdoor for one purpose and not expect others to try and open it," they noted. "People's private messages would be less secure and the real winners would be anyone seeking to take advantage of that weakened security. That is not something we are prepared to do."

Facebook's staunch stand against weakening the encryption of its messenger apps should polish its public image.

"It's really good publicity for them," said Karen North, director of the Annenberg Program on Online Communities at the University of Southern California in Los Angeles.

"This is a good thing for Facebook because it's an announcement that Facebook values our privacy, that it's willing to go to the mat to protect the privacy of each and every one of us," she told TechNewsWorld.

"It's also an announcement that the government can't infiltrate Facebook's encryption," North added, "because if they could, why would they ask for a backdoor?"

Pandora's Door

In theory, a backdoor accessible only to a specific authorized party, like a law enforcement agency, is possible, said Julian Sanchez, a senior fellow with the Cato Institute, a public policy think tank in Washington, D.C.

"As a practical matter, though, Facebook is right," he told TechNewsWorld.

"Implementing secure communications is a hard problem under the best of circumstances, and deliberately designing in functionality for surreptitious interception inherently creates an additional vulnerability that makes an attractive attack surface," Sanchez explained.

"It increases both the risk of technical exploits that malicious hackers might take advantage of," he continued, "and of what we might call 'legal exploits' -- because once such a capability is designed, it will be virtually impossible to make it available to nice democratic governments that respect human rights, while denying it to repressive regimes that criminalize political dissent."

Backdoors affect more than individual privacy.

"When it comes to backdoors, you're talking about a privacy issue, but you're also talking about an infrastructure issue that has really far-reaching implications," said Liz Miller, principal analyst at Constellation Research, a technology research and advisory firm in Cupertino, California.

"We live in a world where people are looking for exploits and ways into the infrastructure of systems every day," she told TechNewsWorld. "If we start to weaken that infrastructure, it's not just the privacy of an individual message that's at risk, it's the privacy of the entire network."

Legislation Needed

Government and law enforcement officials maintain the tech sector is overstating the danger of weakening encryption.

"The single most important criminal justice challenge in the last 10 years is, in my opinion, the use of mobile devices by bad actors to plan, execute, and communicate about crimes," said New York County District Attorney Cyrus R. Vance Jr. in written testimony submitted to the U.S. Senate Judiciary Committee at a hearing on encryption and lawful access held Tuesday.

"Just as ordinary citizens rely on digital communication, so do people involved in terrorism, cyber fraud, murder, rape, robbery, and child sexual assault," he continued.

His office is not anti-encryption, Vance maintained.

"That does not mean encrypted material should be beyond the law when a judge signs a search warrant -- especially when we're talking about evidence tied to a child sex abuse case or a potential terrorist attack," he argued.

It is "unconscionable that smartphone manufacturers, rather than working with government to address public safety concerns, have dug in their heels and mounted a campaign to convince their customers that government is wrong and that privacy is at risk," Vance said.

"Because Apple and Google refuse to reconsider their approach, I believe the only answer is federal legislation ensuring lawful access," he added. "Tech goliaths have shown time and again they have no business policing themselves."

Downside of Lawful Access

There can be hangups, however, with the "lawful access" Vance and others seek.

"The U.S. government can require an American company to install backdoors, but they can't require people to use those backdoored services," the Cato Institute's Sanchez pointed out.

"There are already widely available open source encryption tools with no backdoors, which sophisticated users can switch to if they no longer trust compromised encryption," he continued, "and competing tech companies outside U.S. jurisdiction are sure to eagerly promote their products as an uncompromised, more secure alternative."

In either case, the big loser would be Facebook.

"People utilize WhatsApp because of the encryption," Constellation's Miller observed. "If you take that away, a lot of people will leave the platform, and they'll begin to question whether they want to do business with Facebook."

Support of encryption backdoors by global governments has the security community concerned, observed Kevin Bocek, vice president for security strategy and threat intelligence at Salt Lake City-based Venafi, maker of a platform to protect digital keys and certificates.

"This is not rocket science. Backdoors inevitably create vulnerabilities that can be exploited by cyberattackers. It's understandable that so many security and privacy professionals are concerned. Backdoors are especially appealing to hostile and abusive attackers," he told TechNewsWorld.

"This is a tense moment for technology professionals because they know backdoors make our critical infrastructure and devices more vulnerable. We know that attackers don't abide by restrictions. They don't follow the rules or buy products in controlled markets," Bocek continued.

"Countries that enact these restrictions harm law-abiding businesses and court economic damage," he warned, "as well as intrusions focused on sovereign government processes."