Law enforcement grapples with iPhone's enhanced encryption

October 3 2014, by Julia Love And Robert Salonga, San Jose Mercury News

Apple is no stranger to disruption, having upended the music business with iTunes and the mobile industry with the iPhone. But now, some law enforcement officials are warning that the company is threatening to disrupt their efforts to fight crime.

With its new iOS 8 software, Apple is locking itself out of users' smartphones - and leaving cops and the courts out in the cold. The Cupertino, Calif.-based company recently announced that photos, email, contacts and other information will now be encrypted with users' passcodes, meaning "it's not technically feasible for us to respond to government warrants for the extraction of this data" from the phone. Google followed suit the next day, saying that the forthcoming version of its Android software will offer the same protections.

The software change is a deft way for Apple to underscore its commitment to privacy and distance itself from the shadow cast over Silicon Valley after revelations about the National Security Agency's surveillance programs. But it has triggered some concern from law enforcement officials, and a sharp rebuke from FBI Director James Comey.

"There will come a day - well it comes every day in this business - when it will matter a great, great deal to the lives of people of all kinds that we be able to, with judicial authorization, gain access to a kidnapper's or a terrorist's or a criminal's device," he said Thursday. "I'd hate to have

people look at me and say, 'Well, how come you can't save this kid?'"

To be sure, law enforcement will have other ways to follow a suspect's digital trail. Apple can still share data that people back up from their devices to their Internet-based iCloud accounts, and carriers give investigators call logs and other information gleaned from cell phone towers.

Law enforcement is still gauging how the heightened encryption will affect their investigations. And multiple local law-enforcement sources told the San Jose Mercury News that the new policy is a continuation of ongoing difficulties they have had in getting compliance from Apple while carrying out search warrants involving its customers. They described long delays and a lengthy backlog in responding to law-enforcement requests, but declined to speculate on the reasons behind that occurrence.

San Francisco police offered a measured reaction to the new policy.

"It does make it challenging. But we're not in the business of dictating policy for private companies," spokesman Officer Albie Esparza said. "Although it could impact investigations, there are other ways to obtain information."

Esparza acknowledged that the investigative value of a smartphone has jumped sharply in recent years, calling them "personal lifelines" that could contain a trove of evidence in a suspected crime.

But he said it's too soon to forecast the impact on police work that the security measures will have, particularly with what are known as "exigent circumstances" where a safety emergency spurs one of the exceptions outlined in a U.S. Supreme Court ruling last summer holding that in all but a few cases, warrantless cell phone searches are unconstitutional.

"There will be cases where we'll have to be able to get access, and if we can't, well, we'll cross that bridge when we get there," Esparza said.

A spokesman for Apple declined to comment but cited the company's new privacy policy and a recent conversation Apple CEO Tim Cook had with journalist Charlie Rose. In the interview, Cook stressed that Apple collects minimal data from users because its business is selling devices rather than targeted ads. The company already encrypted iMessages and FaceTime calls with users' passcodes.

Despite concern among some in law enforcement, experts say Apple's move to wall off more information was probably less about thumbing its nose at the U.S. government than extricating itself from criminal investigations in which it has little interest.

"If I'm a private company, that's the last place I want to be," said John Roman, a senior fellow in the Justice Policy Center at the Urban Institute.

But Roman fears that the encryption will pose a huge hurdle, particularly for local law enforcement agencies. With limited forensic capabilities, scanning a smartphone is often one of few convenient options for a local officer to jump-start a case, Roman said.

"On normal, everyday cases, this will be a dead stop for them," he said.

Civil liberties advocates say those concerns are greatly overblown. Hanni Fakhoury, a staff attorney at the Electronic Frontier Foundation, said that although information gleaned from smartphones is often useful, it rarely makes or breaks a case. And though Apple is unable to provide a user's pass code to unlock a phone, he predicts that many suspects will voluntarily supply it, drawing from his experience as a public defender.

"When people are in that interrogation room, they're telling the police, 'Sure, you can open my phone,'" he said.

Fakhoury said it is still unclear whether a judge could order a suspect to open his phone or be held in contempt of court, perhaps foreshadowing a future legal battle.

What's more, experts say Apple users' data will also be more secure as a result of the shift. When companies maintain the ability to circumvent passcodes for law enforcement, hackers can easily abuse the opening, experts say. The safest option is to wall off the information entirely, experts say.

"If you create an access point, both good guys and bad guys can use it," said Bruce Schneier, a computer security and privacy expert.