FBI chief: Apple, Google phone encryption perilous (Update)

September 25 2014, by Ken Dilanian

The FBI director on Thursday criticized the decision by Apple and Google to encrypt smartphones data so it can be inaccessible to law enforcement, even with a court order.

James Comey told reporters at FBI headquarters that U.S. officials are in talks with the two companies. He accused the companies of letting people put themselves beyond the law's reach.

Comey cited child-kidnapping and terrorism cases as two examples of situations where quick access by authorities to information on cellphones can save lives. Comey did not cite specific past cases that would have been more difficult for the FBI to investigate under the new policies, which only involve physical access to a suspect's or victim's phone when the owner is unable or unwilling to unlock it for authorities.

An FBI spokesman Thursday was not able to immediately clarify Comey's remarks.

Both Apple and Google announced last week that their new operating systems will be encrypted, or rendered in code, by default. Law enforcement officials could still intercept conversations but might not be able to access call data, contacts, photos and email stored on the phone.

Even under the new policies, law enforcement could still access a person's cellphone data that has been backed up to the companies' online-storage services. They could also still retrieve real-time phone records

and logs of text messages to see whom a suspect was calling or texting, and they could still obtain wiretaps to eavesdrop on all calls made with the phones.

Comey's criticisms closely tracked complaints earlier this week by Ronald T. Hosko, a former FBI assistant criminal division director who wrote in The Washington Post that Google's and Apple's policies would have resulted in the death of a hostage in a recent North Carolina kidnapping.

The newspaper subsequently corrected Hosko's claims after concluding that the new encryption systems would not have hindered the FBI's rescue of the kidnap victim in Wake Forest, North Carolina. In that case, the FBI pulled telephone records associated with the number used to contact the victim's family for the ransom demand, retrieved other connected toll records and eventually obtained a traditional wiretap to eavesdrop on the kidnappers' conversations and locate and rescue the victim.

The only telephone physically seized in the North Carolina case belonged to a woman accused in the plot, after the hostage was already rescued. Authorities had tried to seize the cell phone from one of the alleged plotters, Kevin Melton, but he smashed it to pieces inside his prison cell on April 9, roughly four hours before the FBI rescued the victim in an Atlanta apartment.

A spokeswoman for Apple and spokesman for Google did not immediately return phone messages from The Associated Press. Google previously said in a statement that its Android phones have offered encryption for three years, but it was being turned on by default in the next release of its operating system.

© 2014 The Associated Press. All rights reserved.

Citation: FBI chief: Apple, Google phone encryption perilous (Update) (2014, September 25) retrieved 3 May 2024 from https://phys.org/news/2014-09-fbi-chief-encryption.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.