CRS Insights

Smartphone Data Encryption: A Renewed Boundary for Law Enforcement?

Kristin Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

October 17, 2014 (IN10166)

Modern-day criminals constantly develop new techniques to facilitate their illicit activities. They have adapted to cross, circumvent, and exploit a number of boundaries—including geographic borders, law enforcement jurisdiction, turf, and cyberspace—which simultaneously present obstacles for the officials tasked with combatting these malicious actors.

In the fast-changing technology space that is today, law enforcement faces a renewed boundary in crime-fighting. According to Attorney General Eric Holder, "[r]ecent technological advances have the potential to greatly embolden online criminals, providing new methods ... to avoid detection."

The Technology Boundary: A Perennial Issue

Technology as a boundary is by no means a new issue for U.S. law enforcement. In the 1990s, for instance, there were "concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance." Specifically, the Government Accountability Office cited the increasing use of digital (including cellular) technologies in public telephone systems as one factor potentially inhibiting the Federal Bureau of Investigation's (FBI's) wiretap capabilities. To help law enforcement maintain the ability to execute authorized electronic surveillance, Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414). Among other things, CALEA required that telecommunications carriers assist law enforcement in executing authorized electronic surveillance. Its requirements have since beenadministratively expanded to apply to broadband Internet access and Voice over Internet Protocol providers. CALEA is not viewed as applying to data contained on smartphones, and there has been "intense debate" about whether it should be expanded to cover this content.

Current Point of Contention

In September 2014, Apple released its latest mobile operating system, iOS 8. In the accompanying privacy policy, Apple noted that personal data stored on devices running iOS 8 are protected by the user's passcode. Moreover,

the company stated, "Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8." Similarly, Google declared that the next version of its Android operating system will include privacy protections—including automatic encryption of data only accessible by entering a valid password, to which Google does not have a key—such that the company will not be able to unlock devices for anyone.

Enhanced data encryption, in part a response to privacy concerns following Edward Snowden's revelations of mass government surveillance, has opened the discussion on how this encryption could impact law enforcement investigations. Law enforcement appears to be generally unnerved by this move. If companies such as Apple and Google do not maintain the ability to unlock certain devices, they cannot turn over information stored *on* the devices to law enforcement—even if the police possess a search warrant. Notably, while law enforcement generally does not need a warrant to search items found on suspects at the time of arrest, the Supreme Court has ruled that this exception does not apply to digital information on cell phones. Nonetheless, the technology companies maintain the ability to turn over information stored *off*the devices in locations such as the "cloud," subject to various statutory restrictions. Law enforcement officials have likened the new encryption to "a house that can't be searched, or a car trunk that could never be opened." There have been concerns that malicious actors, from savvy criminals to terrorists to nation states, may rely upon this very encryption to help conceal their illicit activities. Others, in support of encryption, note that a search warrant is "an instrument of permission, not compulsion." In other words, individuals need not proactively reveal or open hiding places for investigators presenting a search warrant. In addition, some supporting encryption may contend that law enforcement maintains tools to retrieve digital data such as phone records and information stored in the cloud. Encryption proponents may also note that stronger digital security could benefit law enforcement by helping prevent malicious activity including hacking and data breaches.

Going Dark or Going Forward

As experts have noted, "[l]aw enforcement has been complaining about 'going dark' for decades now." The FBI, for instance, established a Going Dark Initiative in an attempt to maintain law enforcement's ability to conduct electronic surveillance in a rapidly changing technology environment. Current questions now involve how, in practice, encryption implemented by technology companies such as Apple and Google may impact law enforcement investigations.

If there is evidence that investigations are hampered or that lives are at risk, as has been suggested may happen, will there need to be some sort of compromise between law enforcement and the technology industry? If so, it seems there may be several paths. One option is that Congress could move to update electronic surveillance laws such that they would cover data stored on smartphones. Relatedly, Congress could act to prohibit the encryption of data without the ability for law enforcement to access the encrypted data. Yet another, non-legislative, option may be for industry and law enforcement to come to a working agreement regarding the sharing of smartphone data.

All of these options may involve the application of a "back door" or "golden key" that can allow for access to smartphones. However, as has been noted, "[w]hen you build a back door ... for the good guys, you can be assured that the bad guys will figure out how to use it as well." This is the tradeoff. Policy makers may debate which is more advantageous for the nation on the whole: (1) increased security coupled with potentially fewer data breaches and possibly greater impediments to law enforcement investigations, or (2) increased access to data paired with potentially greater vulnerability to malicious actors.