Tech

FBI blasts Apple, Google for locking police out of phones

FBI Director James Comey speaking earlier this month. (Chip Somodevilla/Getty Images)

By Craig Timberg and Greg Miller September 25

Follow @craigtimberg Follow @gregpmiller

FBI Director James B. Comey sharply criticized Apple and Google on Thursday for developing forms of smartphone encryption so secure that law enforcement officials cannot easily gain access to information stored on the devices — even when they have valid search warrants.

His comments were the most forceful yet from a top government official but echo a chorus of denunciation from law enforcement officials nationwide. Police have said that the ability to search photos, messages and Web histories on smartphones is essential to solving a range of serious crimes, including murder, child pornography and

attempted terrorist attacks.

“There will come a day when it will matter a great deal to the lives of people … that we will be able to gain access” to such devices, Comey told reporters in a briefing. “I want to have that conversation [with companies responsible] before that day comes.”

Comey added that FBI officials already have made initial contact with the two companies, which announced their new smartphone encryption initiatives last week. He said he could not understand why companies would “market something expressly to allow people to place themselves beyond the law.”

Comey’s remarks followed news last week that Apple’s latest mobile operating system, iOS 8, is so thoroughly encrypted that the company is unable to unlock iPhones or iPads for police. Google, meanwhile, is moving to an automatic form of encryption for its newest version of Android operating system that the company also will not be able to unlock, though it will take longer for that new feature to reach most consumers.

Both companies declined to comment on Comey’s remarks. Apple has said that its new encryption is not intended to specifically hinder law enforcement but to improve device security against any potential intruder.

For detectives working a tough case, few types of evidence are more revealing than a smartphone. Call logs, instant messages and location records can link a suspect to a crime precisely when and where it occurred. And a

The Most Popular All Over

THE ATLANTIC

The Real Reason It's Nearly Impossible to End the Cuba...

SLATE

Video: Ben Affleck Calls Bill Maher’s Views on Islam...

TAMPA BAY TIMES

Richard 'Sandy' Beach, an icon of Alcoholics Anonymous...

surprising number of criminals, police say, like to take selfies posing with accomplices — and often the loot they stole together.

But the era of easy law enforcement access to smartphones may be drawing to a close as courts and tech companies erect new barriers to police searches of popular electronic devices. The result, say law enforcement officials, legal experts and forensic analysts, is that more and more seized smartphones will end up as little more than shiny paperweights, with potentially incriminating secrets locked inside forever.

The irony, some say, is that while the legal and technical changes are fueled by anger over reports of mass surveillance by the National Security Agency, the consequences are being felt most heavily by police detectives, often armed with warrants certifying that a judge has found probable cause that a search of a smartphone will reveal evidence of a crime.

“The outrage is directed at warrantless mass surveillance, and this is a very different context. It’s searching a device with a warrant,” said Orin Kerr, a former Justice Department computer crimes lawyer who is now a professor at George Washington University.

Not all of the high-tech tools favored by police are in peril. They can still seek records of calls or texts from cellular carriers, eavesdrop on conversations and, based on the cell towers used, determine the general locations of suspects. Police can seek data backed up on remote cloud services, which increasingly keep copies of the data

collected by smartphones. And the most sophisticated law enforcement agencies can deliver malicious software to phones capable of making them spy on users.

Yet the devices themselves are gradually moving beyond the reach of police in a range of circumstances, prompting ire from investigators. Frustration is running particularly high at Apple, which made the first announcement about new encryption and is moving much more swiftly than Google to get it into the hands of consumers.

“Apple will become the phone of choice for the pedophile,” said John J. Escalante, chief of detectives for Chicago’s police department. “The average pedophile at this point is probably thinking, I’ve got to get an Apple phone.”

The rising use of encryption is already taking a toll on the ability of law enforcement officials to collect evidence from smartphones. Apple in particular has been introducing tough new security measures for more than two years that have made it difficult for police armed with cracking software to break in. The new encryption is significantly tougher, experts say.

“There are some things you can do. There are some things the NSA can do. For the average mortal, I’d say they’re probably out of luck,” said Jonathan Zdziarski, a forensics researcher based in New Hampshire.

Los Angeles police Detective Brian Collins, who does forensics analysis for anti-gang and narcotics

investigations, says he works on about 30 smartphones a month. And while he still can successfully crack into most of them, the percentage has been gradually shrinking — a trend he fears will only accelerate.

“I’ve been an investigator for almost 27 years,” Collins said, “It’s concerning that we’re beginning to go backwards with this technology.”

The new encryption initiatives by Apple and Google come after June’s Supreme Court ruling requiring police, in most circumstances, to get a search warrant before gathering data from a cellphone. The magistrate courts that typically issue search warrants, meanwhile, are more carefully scrutinizing requests amid the heightened privacy concerns that followed the NSA disclosures that began last year.

Civil liberties activists call this shift a necessary correction to the deterioration of personal privacy in the digital era — and especially since Apple’s introduction of the iPhone in 2007 inaugurated an era in which smartphones became remarkably intimate companions of people everywhere.

“Law enforcement has an enormous range of technical and old-fashioned methods to go after the perpetrators of real crime, and no amount of security effort at Silicon Valley tech companies is going to change that fact,” said Peter Eckersley, director of technology projects at the Electronic Frontier Foundation, a civil liberties group based in San Francisco. “The reality is that if the FBI really wants to investigate someone, they have a spectacular arsenal of weapons.”

Sometimes, police say, that's not enough.

Escalante, the Chicago chief of detectives, pointed to a case in which several men forced their way into the home of a retired officer in March and shot him in the face as his wife lay helplessly nearby. When the victim, Elmer Brown, 73, died two weeks later, city detectives working the case already were running low on useful leads.

But police got a break during a routine traffic stop in June, confiscating a Colt revolver that once belonged to Brown, police say. That led investigators to a Facebook post, made two days after the homicide, in which another man posed in a cellphone selfie with the same gun.

When police found the smartphone used for that picture, the case broke open, investigators say. Though the Android device was locked with a swipe code, a police forensics lab was able to defeat it to collect evidence; the underlying data was not encrypted. Three males, one of whom was a juvenile, eventually were arrested.

"You present them with a picture of themselves, taken with the gun, and it's hard to deny it," said Sgt. Richard Wiser, head of the Chicago violent crimes unit that investigated the case. "It played a huge role in this whole thing. As it was, it took six months to get them. Who knows how long it would have taken without this."

Follow The Post's tech blog, The Switch, where technology and policy connect.

Craig Timberg is a national technology reporter for The Post.

Greg Miller covers the intelligence beat for The Washington Post.