The New York Times | http://nyti.ms/1SFPOpZ

POLITICS | CYBERSECURITY

F.B.I. Director Repeats Call That Ability to Read Encrypted Messages Is Crucial

By NICOLE PERLROTH and DAVID E. SANGER NOV. 18, 2015

The F.B.I. director and the Manhattan district attorney on Wednesday sought to reopen the argument that law enforcement and intelligence officials need to have access to encrypted information on smartphones with court approval.

The question seemed settled last month after President Obama decided not to push legislation requiring American technology companies — notably Apple, Google and Facebook— to roll back smartphone encryption schemes that make it almost impossible to read a target's communications, even if investigators have a court order. But the terrorist attacks in Paris may have changed the politics on both encryption and a range of surveillance issues, with critics renewing their charge that the Obama administration is not using all tools available to stop terrorism.

In a speech at a cybersecurity conference in New York, James B. Comey, who since taking over the F.B.I. has been the most vociferous about the "going dark" problem facing investigators, warned that "we're drifting to a place" where court orders to gain access to text messages or computer communications "are ineffective." Both devices and data in transmission are often encrypted so well that the law enforcement and intelligence agencies cannot crack the coding — and their makers have designed the system so they do not hold the key.

"With lack of cooperation, we are left with 50-foot-high walls on either side,"

Mr. Comey said. “We have to get to a place where we push information to each other at a pace that moves with the speed of the threat.”

He was joined by Cyrus R. Vance, the Manhattan district attorney, who released a 42-page white paper arguing that his office was unable to execute 111 search warrants for smartphones from September 2014 to October 2015 because the devices employed Apple’s “full disk encryption.” That technology prohibits anyone, except the iPhone’s owner, from accessing a device’s contents without a user’s password.

“Last fall, a decision by a single company changed the way those of us in law enforcement work to keep the public safe and bring justice to victims and their families,” the paper said, referring to Apple. “We risk losing crucial evidence in serious cases if the contents of passcode protected smartphones remain immune to a warrant.”

Representatives for Apple did not return requests for comment. In the past, Apple’s chief executive, Timothy Cook, has taken up the other side of the argument, making the case that a way to allow the government access without making the data vulnerable to others simply does not exist.

Aaron Stein, a Google spokesman, said the company, also singled out by the district attorney’s office, declined to comment.

But Bill Conner, president and chief executive of Silent Circle, a firm that sells software to encrypt cellphone conversations and a “Blackphone” that encrypts almost all smartphone activity, said Mr. Comey was looking to return to an era that was over. “The reality is, we have to encrypt more data to keep the bad guys out,” Mr. Conner said, noting the series of recent breaches that allowed Chinese hackers to get the security records of 22 million Americans with security clearances, including Mr. Comey himself.

Mr. Vance’s report argued that law enforcement officials should not seek a “back door” to get inside encrypted phones, but rather a roll back to Apple’s previous encryption methodology. Until roughly a year ago, the company kept the

key to unlock customers' communications in the event it received a court order.

But its newest encryption system, part of its operating system, keeps iPhone data secure even from Apple. The company no longer holds the keys; customers do. Google switched on a similar system as the default in Android phones last year, though not every Android manufacturer turns the encryption on by default.

Apple and Google have said they always planned to move to full disk encryption schemes, largely to keep pace in the longstanding cat-and-mouse game with cybercriminals. But the timing of their moves — after disclosures by Edward J. Snowden, the former N.S.A. contractor — suggested that the companies were reacting to disclosures that some critics said made them government collaborators.

Mr. Comey said in his speech that encryption technology was already in use by the Islamic State. He argued that recruiters for the extremist group used unencrypted messages to reach out to prospective members, then switched to encrypted methods once they netted a good prospect. But American and French officials have said they have no definitive evidence to back up claims that the terrorists behind Friday's attacks used encrypted communications.

The French news media reported on Wednesday that the predawn raids in the Paris suburb of St.-Denis were prompted by the discovery of a mobile phone with unencrypted contents that was discovered by investigators in a trash can near the Bataclan concert hall. Contrary to warnings that encryption has left investigators in the dark, in this case, French officials were able to easily access a detailed plan of the Bataclan assault and an unencrypted text message sent at 9:42 p.m. on Friday that said, "On est parti on commence," which roughly translates as, "Here we go, we're starting."

Some security experts and cryptographers said some officials were trying to use the Paris attacks to push their agenda.

"What you're now seeing is the two-day impulse response," said Ross Anderson, a professor of security engineering at Cambridge University. "Never waste a good crisis, as they say."

J. David Goodman contributed reporting.

A version of this article appears in print on November 19, 2015, on page A17 of the New York edition with the headline: F.B.I. Director Repeats Call That Ability to Read Encrypted Messages Is Crucial.
