The New York Times | http://nyti.ms/1neKX4p

THE DROP
NOW PLAYING
GET TICKETS

TECHNOLOGY | NYT NOW

Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.

By DAVID E. SANGER and BRIAN X. CHEN SEPT. 26, 2014

WASHINGTON — Devoted customers of Apple products these days worry about whether the new iPhone 6 will bend in their jean pockets. The National Security Agency and the nation's law enforcement agencies have a different concern: that the smartphone is the first of a post-Snowden generation of equipment that will disrupt their investigative abilities.

The phone encrypts emails, photos and contacts based on a complex mathematical algorithm that uses a code created by, and unique to, the phone's user — and that Apple says it will not possess.

The result, the company is essentially saying, is that if Apple is sent a court order demanding that the contents of an iPhone 6 be provided to intelligence agencies or law enforcement, it will turn over gibberish, along with a note saying that to decode the phone's emails, contacts and photos, investigators will have to break the code or get the code from the phone's owner.

Breaking the code, according to an Apple technical guide, could take "more than 5 1/2 years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers." (Computer security experts question that figure, because Apple does not fully realize how quickly the N.S.A. supercomputers can crack codes.)

Already the new phone has led to an eruption from the director of the F.B.I., James B. Comey. At a news conference on Thursday devoted largely to combating terror threats from the Islamic State, Mr. Comey said, "What concerns me about this is companies marketing something expressly to allow

people to hold themselves beyond the law."

He cited kidnapping cases, in which exploiting the contents of a seized phone could lead to finding a victim, and predicted there would be moments when parents would come to him "with tears in their eyes, look at me and say, 'What do you mean you can't' " decode the contents of a phone.

"The notion that someone would market a closet that could never be opened — even if it involves a case involving a child kidnapper and a court order — to me does not make any sense."

Apple declined to comment. But officials inside the intelligence agencies, while letting the F.B.I. make the public protests, say they fear the company's move is the first of several new technologies that are clearly designed to defeat not only the N.S.A., but also any court orders to turn over information to intelligence agencies. They liken Apple's move to the early days of Swiss banking, when secret accounts were set up precisely to allow national laws to be evaded.

"Terrorists will figure this out," along with savvy criminals and paranoid dictators, one senior official predicted, and keep their data just on the iPhone 6. Another said, "It's like taking out an ad that says, 'Here's how to avoid surveillance — even legal surveillance.' "

The move raises a critical issue, the intelligence officials say: Who decides what kind of data the government can access? Until now, those decisions have largely been a matter for Congress, which passed the Communications Assistance for Law Enforcement Act in 1994, requiring telecommunications companies to build into their systems an ability to carry out a wiretap order if presented with one. But despite intense debate about whether the law should be expanded to cover email and other content, it has not been updated, and it does not cover content contained in a smartphone.

At Apple and Google, company executives say the United States government brought these changes on itself. The revelations by the former N.S.A. contractor Edward J. Snowden not only killed recent efforts to expand the law, but also made nations around the world suspicious that every piece of American hardware and software — from phones to servers made by Cisco Systems — have "back doors" for American intelligence and law enforcement.

Surviving in the global marketplace — especially in places like China, Brazil and Germany — depends on convincing consumers that their data is secure.

Timothy D. Cook, Apple's chief executive, has emphasized that Apple's core business is to sell devices to people. That distinguishes Apple from companies that make a profit from collecting and selling users' personal data to advertisers, he has said.

This month, just before releasing the iPhone 6 and iOS 8, Apple took steps to underscore its commitment to customer privacy, publishing a revised privacy policy on its website.

The policy described the encryption method used in iOS 8 as so deep that Apple could no longer comply with government warrants asking for customer information to be extracted from devices. "Unlike our competitors, Apple cannot bypass your passcode, and therefore cannot access this data," the company said.

Under the new encryption method, only entering the passcode can decrypt the device. (Hypothetically, Apple could create a tool to hack into the device, but legally the company is not required to do that.)

Jonathan Zdziarski, a security researcher who has taught forensics courses to law enforcement agencies on collecting data from iPhones, said to think of the encryption system as a series of lockers. In the older version of iOS, there was always at least one locker that was unlocked, which Apple could enter to grab certain files like photos, call history and notes, in response to a legal warrant.

"Now what they're saying is, 'We stopped using that locker,' " Mr. Zdziarski said. "We're using a locker that actually has a combination on it, and if you don't know the combination, then you can't get inside. Unless you take a sledgehammer to the locker, there's no way we get to the files."

The new security in iOS 8 protects information stored on the device itself, but not data stored on iCloud, Apple's cloud service. So Apple will still be able to obtain some customer information stored on iCloud in response to government requests.

Google has also started giving its users more control over their privacy. Phones using Google's Android operating system have had encryption for three years. It is not the default setting, however, so to encrypt their phones, users

have to go into their settings, turn it on, and wait an hour or more for the data to be scrambled.

That is set to change with the next version of Android, set for release in October. It will have encryption as the default, "so you won't even have to think about turning it on," Google said in a statement.

A Google spokesman declined to comment on Mr. Comey's suggestions that stronger encryption could hinder law enforcement investigations.

Mr. Zdziarski said that concerns about Apple's new encryption to hinder law enforcement seemed overblown. He said there were still plenty of ways for the police to get customer data for investigations. In the example of a kidnapping victim, the police can still request information on call records and geolocation information from phone carriers like AT&T and Verizon Wireless.

"Eliminating the iPhone as one source I don't think is going to wreck a lot of cases," he said. "There is such a mountain of other evidence from call logs, email logs, iCloud, Gmail logs. They're tapping the whole Internet."

David E. Sanger reported from Washington, and Brian X. Chen from San Francisco. Conor Dougherty contributed reporting from San Francisco.

A version of this article appears in print on September 27, 2014, on page A1 of the New York edition with the headline: Signaling Post-Snowden Era, New iPhone Locks Out N.S.A..

© 2014 The New York Times Company