16099 Why Apple Is Right to Challenge an Order to Help the F.B.I.

NYT, By THE EDITORIAL BOARD FEB. 18, 2016

In an order issued on Tuesday, Magistrate Judge Sheri Pym said Apple must create new software that would bypass security features on the iPhone used by the terrorist, Syed Rizwan Farook. That would allow the Federal Bureau of Investigation to unlock the device and retrieve the pictures, messages and other data on it.

Law enforcement agencies have a legitimate need for evidence, which is all the more pressing in terrorism cases. But the Constitution and the nation's laws limit how investigators and prosecutors can collect evidence.

Apple has already given the F.B.I. data from the phone that was backed up and stored on its iCloud service. But the company's chief executive, Timothy Cook, has said that requiring it to create software to bypass a feature that causes the phone to erase its data if 10 incorrect passwords are entered would set a dangerous precedent and could undermine the security of its devices. The Department of Justice has argued that the software would be used on that phone only and notes that Apple has previously helped law enforcement unlock phones. The company changed how it encrypts phones after the surveillance revelations by Edward Snowden.

But writing new code would have an effect beyond unlocking one phone. If Apple is required to help the F.B.I. in this case, courts could require it to use this software in future investigations or order it to create new software to fit new needs. It is also theoretically possible that hackers could steal the software from the company's servers.

Even if the government prevails in forcing Apple to help, that will hardly be the end of the story. Experts widely believe that technology companies will eventually build devices that cannot be unlocked by company engineers and programmers without the permission of users. Newer smartphones already have much stronger security features than the iPhone 5c Mr. Farook used.

Some officials have proposed that phone and computer makers be required to maintain access or a "back door" to encrypted data on electronic devices. In October, the Obama administration said it would not seek such legislation, but the next president could have a different position.

Congress would do great harm by requiring such back doors. Criminals and domestic and foreign intelligence agencies could exploit such features to conduct mass surveillance and steal national and trade secrets. There's a very good chance that such a law, intended to ease the job of law enforcement, would make private citizens, businesses and the government itself far less secure.

416 words