

Police: New Apple technology will delay justice in DC area



By Megan Cloherty (<http://wtop.com/author/megan-cloherty/>) | @ClohertyWTOP
(<https://twitter.com/ClohertyWTOP>)
September 13, 2017 4:54 am



Apple's announcement of facial recognition technology security and an increasingly secure operating system will present significant challenges to law enforcement tasked with accessing devices to find criminal evidence. (AP Photo/Marcio Jose Sanchez, File)

WASHINGTON — Apple's new security features will make it harder for local police to retrieve digital evidence they need to solve crimes.

While great for consumers, without the ability to bypass enhanced security such as facial recognition, investigators said it will delay justice.

“Face ID is the future of how we unlock our smartphones and protect our sensitive information,” said Apple senior Vice President of Marketing Phil Schiller during [the tech giant’s announcement \(http://wtop.com/consumer-news/2017/09/the-latest-apple-may-bring-facial-recognition-to-mainstream/\)](http://wtop.com/consumer-news/2017/09/the-latest-apple-may-bring-facial-recognition-to-mainstream/) Tuesday, Sept. 12.

But as Apple fans delighted in the new suite of products including the debut of the iPhone X, law enforcement let out a collective sigh.

“It’s very frustrating for law enforcement because it makes our job much more difficult to support the community,” said Detective Jason Friedman, who works in the Fairfax County Police computer forensics department. The biggest issue, he said, is the latest operating system, IOS 11.

“Most of the forensics community in law enforcement has known for a while, through the Apple IOS 11 betas, that security was going to be even more difficult and hamper law enforcement’s ability to extract data,” he said. He did not elaborate on the specific change in the security features that further complicates extraction of data.

WTOP broke the story in July that investigators across Maryland are [experiencing monthslong backlogs \(http://wtop.com/maryland/2017/07/delayed-evidence-in-charles-co-case-sheds-light-on-state-crime-lab-backlog/\)](http://wtop.com/maryland/2017/07/delayed-evidence-in-charles-co-case-sheds-light-on-state-crime-lab-backlog/) in digital forensic labs because of the time it takes to comb through the tremendous volume of evidence contained on any single device.

However, if investigators cannot access the phone’s data, or are delayed in doing so, justice could be on hold indefinitely.

That’s currently the situation with a case investigators are working on in Fairfax County.

“There was actually an iPad and we couldn’t get into it, and it’s a very serious case ... We’re going to have wait for a method, if there ever is one, in order to bypass the security to obtain data from the iPad,” Friedman said. He could not elaborate on the nature of the crime.

Working off a search warrant or court order, digital forensic analysts access devices looking for evidence such as photos and videos, GPS location data and message history while investigating cases ranging from homicides to traffic crashes.

“Within the last couple weeks we’ve had an iPhone 6S and an iPhone 7 in here where it was pass code protected. There was no way to bypass that security and we could not obtain data from the cellphone,” he said in another example.

At the computer evidence recovery section of Virginia State Police, First Sgt. Rob Keeton said sometimes the evidence analysts can pull off an iPhone 7 is “slim to none,” depending on what data analysts have court permission to access.

The unit has a four-month backlog in processing digital evidence, Keeton said, which could only grow longer with the introduction of technology that’s harder to crack.

Encrypted devices present a challenge for law enforcement nationwide. The issue found a national spotlight in 2016 as FBI agents investigated the [attacks in San Bernadino, California \(http://wtop.com/news/2015/12/san-bernardino-attack-a-look-at-the-shooting-investigation/\)](http://wtop.com/news/2015/12/san-bernardino-attack-a-look-at-the-shooting-investigation/).

“Apple has spent an enormous amount of energy to secure our devices from unauthorized users, as this battle is clearly showing, but it could include your family after you pass. Apple does not store a phone’s lock code, and without it, accessing the information on a device becomes extremely complex, if not impossible,” tech expert and Data Doctor [Ken Colburn wrote for WTOP \(http://wtop.com/tech/2016/02/column-lessons-everyone-apple-vs-fbi/\)](http://wtop.com/tech/2016/02/column-lessons-everyone-apple-vs-fbi/) following the legal debate over the deceased terrorist’s locked phone.

It is not just the security of new Apple products that present an obstacle for law enforcement. Friedman said some Samsung phones are encrypted right out of the box, making it difficult to extract data. And, while Apple allows users to delay operating system updates, Friedman said eventually they are pushed to older devices, rendering them impenetrable.

On the heels of the massive [Equifax data breach \(http://wtop.com/business-finance/2017/09/equifax-breach-sows-chaos-among-143m-americans/\)](http://wtop.com/business-finance/2017/09/equifax-breach-sows-chaos-among-143m-americans/) that compromised an estimated 143 million Americans’ vital personal and financial data, many consumers will likely welcome a more secure cellphone.

“While they have their right of privacy, unfortunately their right of privacy also hinders our ability to solve the crime and find who could possibly be their murderer,” Friedman said.

It's unclear how the new facial recognition technology will increase the current backlog at a majority of departments in the D.C. region, but forensic analysts said as of now, there is no silver bullet to access the encrypted operating system that will be prevalent on consumer devices within a matter of months.

Like WTOP on [Facebook](https://www.facebook.com/wtopnews) (<https://www.facebook.com/wtopnews>) and follow [@WTOP](https://twitter.com/WTOP) (<https://twitter.com/WTOP>) on Twitter to engage in conversation about this article and others.

© 2017 WTOP. All Rights Reserved.

IN OTHER NEWS:

McMaster, Tillerson: Trump is out of Paris Climate Accord, but 'the door is open'



Copyright © 2017 by WTOP. All rights reserved.

- [Feedback](http://wtop.com/feedback/) (<http://wtop.com/feedback/>)
- [Privacy Policy](http://corporate.hubbardradio.com/privacy-policy/) (<http://corporate.hubbardradio.com/privacy-policy/>)
- [Terms of Use](http://corporate.hubbardradio.com/terms-of-use/) (<http://corporate.hubbardradio.com/terms-of-use/>)
- [Copyright](http://wtop.com/copyright/) (<http://wtop.com/copyright/>)
- [EEO](http://wtop.com/wp-content/uploads/2017/05/6_1_2017Wash-DC-Market.pdf) (http://wtop.com/wp-content/uploads/2017/05/6_1_2017Wash-DC-Market.pdf)
- [Hubbard Radio](http://corporate.hubbardradio.com/) (<http://corporate.hubbardradio.com/>)
- [FCC Public Inspection File](http://wtop.com/wtop-103-5-fm-wwwt-107-7-fm-wt1p-103-9-fm-wwfd-820-am-online-fcc-public-inspection-files/) (<http://wtop.com/wtop-103-5-fm-wwwt-107-7-fm-wt1p-103-9-fm-wwfd-820-am-online-fcc-public-inspection-files/>)