The Washington Post

Apple is making it harder for police to collect evidence from iPhones of suspected criminals

Craig Timberg and Tony Romm

June 13, 2018

Apple announced Wednesday that it would block access to a port that law enforcement uses to break into iPhones during criminal investigations, a move that could reignite debate over whether tech companies are doing enough to help authorities probing serious crimes.

Apple said the change, which would disable the Lightning port on the bottom of iPhones an hour after users lock their phones, is part of software updates to be rolled out in the fall. Designed to better protect the private information of iPhone users, it will have little obvious effect on most people using the devices but will make it far more difficult for investigators to use extraction tools that attach through the port to collect the contents of seized iPhones.

The change is not intended to thwart law enforcement efforts, Apple said. "We're constantly strengthening the security protections in every Apple product to help customers defend against hackers, identity thieves and intrusions into their personal data," the company said in a statement. "We have the greatest respect for law enforcement, and we don't design our security improvements to frustrate their efforts to do their jobs."

Yet some authorities almost certainly will see it as yet another barrier to carrying out their legally sanctioned investigations.

Apple has been at the center of such debates since it declined FBI requests to unlock an iPhone 5C used by a gunman in the San Bernardino shooting in 2015 that left 14 people dead.
A brewing legal showdown was defused when the FBI hired professional hackers to crack into the device. Many such efforts rely on gaining access through the Lightning for which Apple is now restricting access.

The Lightning port is used for charging iPhones, which will still be possible when the devices are in their locked state, and for transferring data, which will be blocked after an hour. Police sometimes seek to extract content by connecting devices to iPhone ports many days after seizing them from users under investigation.

Reaction to the proposed change broke along familiar lines, with privacy and security advocates cheering the move and law enforcement officials decrying it.

"This could be painted as fundamentally about denying law enforcement access, but this is a security vulnerability," said Julian Sanchez, a senior fellow at the Cato Institute. "There is a method by which the security of the [iPhone] can be compromised by devices law enforcement can purchase. There's not really any reason to think only law enforcement will ever have those devices."

The spread of popular consumer devices with access to user communications, photos, documents, call records and location histories proved to be a massive boon for law enforcement and intelligence services for years. But revelations about the volume and precision of such data — most famously from former National Security Agency contractor Edward Snowden in 2013 — prompted a consumer backlash. Companies responded with a wave of encryption initiatives and other security improvements on computers, smartphones and popular communication tools such as email.

Apple was among the leaders of this movement, portraying its devices as more secure than those of rivals and presenting its business model — which relied on pricey products, not the personal data of its users, for profit — as more attuned to the privacy expectations of its customers. The company drew particular ire from law enforcement in 2014 when it announced that its iOS 8 mobile operating system would include a form of encryption making it impossible for the company to turn over the contents of iPhones to police — even when they had search warrants.

FBI officials in particular have complained about what they call the "going dark" problem as encryption becomes increasingly widespread and robust across a range of consumer devices and services.

"I think that privacy protections are on a collision course with responsible law enforcement actions to conduct legitimate investigations," said Ronald Hosko, a former assistant director of the FBI who is now president of the Law Enforcement Legal Defense Fund, which raises money to defend officers accused of misconduct. "Terrorists or other criminal organizations will do something that's heinous, in a way that is blocked from lawful law enforcement view. They will to some extent get away with it. We will lose lives, we will lose infrastructure in a big way, and then we will be having a different conversation."

For months, the FBI has been criticized for understating its ability to break into encrypted devices. In March, an inspector general for the Justice Department found that federal law enforcement officials "did not pursue all possible avenues" to break into the iPhone of the San Bernardino attacker.

The Washington Post reported in May that the FBI had overstated by thousands the number of mobile devices to which it could not gain access because of encryption.

Privacy advocates have noted that personal data backed up to cloud services, such as Apple's iCloud, has become a popular target for investigators as devices themselves have become better protected. Malicious hackers also have exploited such cloud-based backups to collect user information and photographs.

"It's good that Apple continues to improve the security of the devices it gets against unauthorized access and hacking," said Peter Eckersley, chief computer scientist for the Electronic Frontier Foundation, a civil liberties group based in San Francisco. "But it remains the case that iCloud backups are a huge loophole in Apple's device security, and most of what people do on their iPhones and iPads is available to law enforcement."