US hacks iPhone, ends legal battle but questions linger (Update)

March 29 2016, by Tami Abdollah And Brandon Bailey

In this Friday, Sept. 25, 2015, file photo, an Apple iPhone 6s Plus smartphone is displayed at the Apple store at The Grove in Los Angeles. The FBI said Monday, March 28, 2016, it successfully used a mysterious technique without Apple Inc.'s help to hack into the iPhone used by a gunman in a mass shooting in California, effectively ending a pitched court battle between the Obama administration and

one of the world's leading technology companies. (AP Photo/Ringo H.W. Chiu, File)

The extraordinary legal fight pitting the Obama administration against technology giant Apple Inc. ended unexpectedly after the FBI said it used a mysterious method without Apple's help to hack into a California mass shooter's iPhone.

Left unanswered, however, were questions about how the sudden development would affect privacy in the future, and what happens the next time the government is frustrated by digital security lockout features.

Government prosecutors asked a federal judge on Monday to vacate a disputed order forcing Apple to help the FBI break into the iPhone, saying it was no longer necessary.

The FBI used the unspecified technique to access data on an iPhone used by gunman Syed Farook, who died with his wife in a gun battle with police after they killed 14 people in San Bernardino, California, in December. The Justice Department said agents are now reviewing the information on the phone.

But the government's brief court filing, in U.S. District Court for the Central District of California, provided no details about how the FBI got into the phone. Nor did it identify the non-government "outside party" that showed agents how to get past the phone's security defenses. Authorities had previously said only Apple had the ability to help them unlock the phone.

Apple responded by saying it will continue to increase the security of its

products.

Read: Explainer: Apple vs. FBI—What Happened?

"We will continue to help law enforcement with their investigations, as we have done all along," the company added in a statement, while reiterating its argument that the government's demand for Apple's help was wrong.

"This case should never have been brought," the company said.

FBI Assistant Director David Bowdich said Monday that examining the iPhone was part of the authorities' effort to learn if the San Bernardino shooters had worked with others or had targeted any other victims. "I am satisfied that we have access to more answers than we did before," he said in a statement.

The dispute had ignited a fierce Internet-era national debate that pitted digital privacy rights against national security concerns and reinvigorated discussion over the impact of encryption on law enforcement's ability to serve the public.

Rep. Darrell Issa, R-California, said in a statement that while it was "preferable" that the government gained access to the iPhone without Apple's help, the fundamental question of the extent to which the government should be able to access personal information remains unanswered.

Issa, a critic of the administration's domestic surveillance practices, said the government's legal action against Apple raised constitutional and privacy questions and that "those worried about our privacy should stay wary" because this doesn't mean "their quest for a secret key into our devices is over."

The surprise development punctured the temporary perception that Apple's security might have been good enough to keep consumers' personal information safe even from the U.S. government.

And while the Obama administration created a policy for disclosing such security vulnerabilities to companies, the policy allows for a vulnerability to be kept secret if there is a law enforcement or national security rationale for doing so.

The withdrawal of the court process also takes away Apple's ability to legally request details on the method the FBI used in this case. Apple attorneys said last week that they hoped the government would share that information with them if it proved successful.

The Justice Department wouldn't comment on any future disclosure of the method to Apple or the public.

Denelle Dixon-Thayer, chief legal and business officer at Mozilla, which makes the Firefox web browser, said in a statement that "fixing vulnerabilities makes for better products and better security for everyone" and the "government needs to take that into account" and disclose the vulnerability to Apple.

Jay Kaplan, a former NSA computer expert who's now CEO of cyber-security firm Synack, said it is likely Apple will pursue avenues to further lock down their operating systems and hardware, especially as a result of the public announcement of some new technique to crack their phones.

U.S. Magistrate Sheri Pym of California last month ordered Apple to provide the FBI with software to help it hack into Farook's work-issued iPhone. The Justice Department relied on a 1789 law to argue it had the authority to compel Apple to bypass its security protocols on its phone

for government investigators. While Magistrate Judge James Orenstein in New York ruled last month in a separate case that the U.S. was seeking broad powers under that legal argument, the decision wasn't binding in the California case and the Justice Department is appealing.

Technology and civil liberties organizations say they're concerned the case is far from settled, with some worrying that smaller companies might not have the resources to fight off similar demands.

Apple CEO Tim Cook had argued that helping the FBI hack the iPhone would set a dangerous precedent, making all iPhone users vulnerable, if Apple complied with the court order. He as well as FBI Director James Comey has said that Congress needs to take up the issue.

Apple was headed for a courtroom showdown with the government last week, until federal prosecutors abruptly asked for a postponement so they could test a potential solution brought to them by a party outside of the U.S. government last Sunday.

The encrypted phone was protected by a passcode that included security protocols: a time delay and auto-erase featured that destroyed the phone's data after 10 tries. The two features made it impossible for the government to repeatedly and continuously test passcodes in what's known as a brute-force attack. But with those features removed, the FBI said it would take 26 minutes to crack the phone.

A law enforcement official said the FBI would continue to aid its local and state partners with gaining evidence in cases—implying that the method would be shared with them. The official spoke to reporters on condition of anonymity because he wasn't authorized to publicly comment.

High on the waiting list for assistance likely is Manhattan District

Attorney Cyrus Vance, who told a U.S. House panel earlier this month that he has 205 iPhones his investigators can't access data from in criminal investigations. Apple is also opposing requests to help extract information from 14 Apple devices in California, Illinois, Massachusetts and New York.