FBI wins court order forcing Apple to install backdoor in iPhone security systems

Thomas Gaist
18 February 2016

The Obama administration secured a court order from a California-based federal judge on Tuesday to force tech giant Apple to develop special software designed to compromise encryption security features embedded in the iPhone's iOS 9 operating system.

The court decision, utilizing an obscure and antidemocratic law from the 18th century, is part of efforts to utilize last year's attack in San Bernardino, California to intensify the assault on democratic rights and expand the police-state spying powers of the government.

The FBI and the Justice Department claim that the new software is necessary to enable federal investigators to search through an iPhone belonging to Syed Rizwan Farook, one of the attackers responsible for the mass shooting at the Inland Regional Center in San Bernardino.

At stake, however, is far more than the data on Farook's phone. The government wants broad authority to bypass encryption mechanisms on any communications that it is not presently able to monitor.

US agents have been unable to access Farook's phone as a result of Apple's built-in "auto-erase" feature, which deletes the smartphone's data after ten or more incorrect attempts to unlock it. The phone's security features prevent the agency from employing its preferred method of "brute forcing" entry, i.e., trying every possible password.

Judge Sheri Pym of the Federal District Court for the District of Central California ruled Tuesday that Apple must find a way to "bypass and disable" the security features on Farook's phone. Apple will appeal the ruling within days, and the case could be decided in the Supreme Court.

Government attorneys claim that the ruling compels Apple to design software that can penetrate the iPhone's data protection systems, citing a statute known as the All Writs Act, which allows judges to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." The administration has adopted a broad interpretation of the law that effectively allows the courts to overrule constitutional limitations on state powers.

White House, spokesman Josh Earnest said on Wednesday that the Justice Department and the FBI have the Obama administration's "full support."

The ruling is only the latest stage in the efforts of the Obama administration and the political establishment to use the attacks in San Bernardino to counter the widespread opposition to domestic spying that followed the revelations of NSA whistleblower Edward Snowden. Along with the terror attacks in Paris, the events in southern California have become the central pretext for a new expansion of the US government's mass surveillance programs.

Snowden spoke out against the FBI assault on encryption Wednesday, describing the events as "the most important tech case in a decade."

"The FBI is creating a world where citizens rely on Apple to defend their rights," Snowden said in a tweet.

Apple, Google, Yahoo, Facebook and other leading firms entered into secret contracts with the US government from the mid-2000s onward, giving the NSA access to electronic communications data stored on their servers, as revealed in NSA documents released by Snowden beginning in the summer of 2013. The documents also showed that the NSA had set up numerous illegal and unconstitutional programs that seek to monitor all telephone records, emails and other communications in the US and internationally.

Pointing to the broad implications of the ruling in a

© World Socialist Web Site

letter released on Wednesday, Apple CEO Tim Cook described the government's request as "unprecedented," saying that the technology demanded by the FBI could be used against hundreds of millions of devices.

"It would be the equivalent of a master key," Cook wrote. "Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features."

"The government is asking Apple to hack our own users," Cook wrote. The spy software could be used to "intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge." The software hack would "have the potential to unlock any iPhone in someone's physical possession."

However, lest there be any doubt about Apple's allegiance to the intelligence establishment and its "war on terror," Cook went on to insist that Apple has "done everything that is both within our power and within the law to help [the FBI]."

"When the FBI has requested data that's in our possession, we have provided it," Cook wrote. "We have great respect for the professionals at the FBI, and we believe their intentions are good."

Apple's opposition to the FBI's anti-encryption drive flows from the material interests of its shareholders. Apple is engaged in a competitive struggle for market share on a world scale and stands to lose business, both from consumers and from foreign governments, if it is perceived as being completely penetrated by the US spy apparatus.

According to an article in the *New York Times*, Apple had "hoped to resolve the impasse without having to rewrite their own encryption software." The company was "frustrated by the Justice Department's refusal to file its demands under seal rather than airing them in court, according to an industry executive with knowledge of the case." In other words, because the request became publicly known, the company felt compelled to release a statement opposing the ruling.

Intelligence agencies have been pressing for legislation to bypass encryption mechanisms since long before the San Bernardino attacks. FBI Director James Comey has agitated for new laws requiring the installation of "backdoor" access to encryption technology almost continuously since taking office. The attacks, however, were immediately used to escalate the "war on terror campaign" and shift the entire political establishment to the right.

One of the possible outcomes of the dispute with Apple is the passage of legislation in Congress that would explicitly authorize the government to force companies to give it access to text messages and other encrypted data on cell phones. Leading Democrats and Republicans in Congress moved quickly to back the court decision and criticize Apple for opposing it.

The basic target of these moves—as with the police-state spying apparatus as a whole—is not the Islamic State or Al Qaeda, but all opposition to the American ruling class's policy of war and social reaction. As the United States prepares for a massive escalation of military violence, it is at the same time intensifying the assault on democratic rights at home.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site