White House steps up drive to outlaw encryption

Andre Damon
19 February 2016

The court order to force technology company Apple Inc. to create a "backdoor" to its iOS mobile operating system is a substantial new offensive in the US government's drive to spy on the data and communications of everyone in the world.

The ruling comes as the Senate Intelligence Committee is preparing to introduce a bill that would create criminal penalties for companies that do not comply with court orders to decipher encrypted communications, the *Wall Street Journal* reported Thursday.

On Tuesday, Magistrate Judge Sheri Pym of the US District Court for the District of Central California ordered Apple to create a fraudulent software update that intelligence agencies could use to access encrypted data on the company's mobile telephones and tablets.

Formally, the order stipulates that Apple must provide "technical assistance" to the Federal Bureau of Investigation in hacking an Apple iPhone seized while executing a search warrant into the car owned by Tafsheen Malik, one of the shooters in the December 2, 2015 mass killing in San Bernardino, California.

But as Apple chief executive Timothy D. Cook made clear in an open letter published Wednesday, the ruling would create a technical and legal precedent for the government to hack into phones on demand.

The ruling is another step toward the US intelligence agencies' goals of being able to intercept and monitor all data stored or transmitted anywhere in the world, or to, "sniff it all, collect it all, know it all, process it all and exploit it all," as one internal document leaked by Edward Snowden put it.

Pym's order is a pseudo-legal travesty. It is based on a false reading of the All Writs Act of 1789, which states that the courts may issue orders "agreeable to the usages and principles of law." Pym's ruling simply ignores this latter clause and interprets the act to mean that the courts are given effective plenipotentiary powers to do whatever they declare "necessary or appropriate." This is simply a prostitution of the judiciary to grant the executive branch effectively unlimited spying powers.

As Cook notes, "The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software 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."

In this case, the ruling would require the world's largest technology company to "hack our own users and undermine decades of security advancements that protect...tens of millions of American citizens."

The ruling mandates Apple to create a version of the iOS operating system with key security features disabled, and then create a false digital signature certifying the operating system as genuine in order to install it onto the phone in question. This would then allow the Federal Bureau of Investigation to carry out a "brute force" hack of the phone's password in order to gain access to the phone's data.

Once such software is created, there is no way to prevent it from being used at will by intelligence agencies.

The ruling is the latest stage in the Obama administration's drive to expand government spying in the wake of Edward Snowden's 2013 revelations of mass illegal government surveillance. In May 2015, Congress passed the USA Freedom Act, which was

designed to give the veneer of ending illegal government surveillance while in reality allowing it to continue in slightly modified form.

In the wake of the November 2015 terror attacks in Paris and the December mass shooting in San Bernardino, the White House shifted to the offensive, demanding that electronics and computer manufacturers create backdoors to encryption.

This is entirely in keeping with the Obama administration's record on democratic rights. The Obama White House has carried out twice as many prosecutions of reporters and whistleblowers for leaking classified information than all previous administrations combined, including the jailing of Chelsea Manning and the witch hunts of Edward Snowden and WikiLeaks founder Julian Assange.

The Obama White House has refused to prosecute those within the Bush administration responsible for torture, and instead conspired with CIA Director John Brennan, whom Obama appointed, to suppress the Senate Intelligence Committee torture report. The administration then defended Brennan when his hacking into Senate Intelligence Committee staffers' computers was exposed.

This is in addition to having been the first president to claim the right to kill American citizens, including inside the borders of the United States, without a trial. To date, the White House's drone murder program has led to the deaths of thousands of people in Pakistan, Yemen and other countries, including at least four American citizens.

Now, amid an intensification of its wars in the Middle East and on the threshold of a potential conflict with Russia and China, the White House is seeking to clamp down on encrypted communications in order to threaten and intimidate popular opposition to war, attacks on democratic rights and social inequality.

No one should be under any illusion that corporations such as Apple, who have collaborated with illegal spying in the past and whose qualms now are based on financial considerations, will be either willing or able to mount a successful effort to restrain the drive to criminalize encryption.

The defense of democratic rights requires the building of a mass movement of the working class in opposition to war and social inequality, armed with the socialist program of reorganizing society to meet social need, not private profit.