The assault on encryption and the drive to expand police state spying

Joseph Kishore
24 February 2016

With its highly public court battle with Apple over access to an encrypted phone, the Obama administration is very deliberately seeking to create the framework for a massive expansion of police state spying powers in the United States.

The claim by White House officials, backed Tuesday by Microsoft founder Bill Gates, that what is involved is a single case involving one phone—the smartphone used by one of the shooters in last year's San Bernardino attack—is a lie aimed at covering up the government's intentions.

Supporting the Obama administration, Gates said in an interview with the *Financial Times* that a February 16 court order requiring Apple to help the FBI access a phone used by Syed Rizwan Farook was "a specific case where the government is asking for access to information." He added, "They are not asking for some general thing, they are asking for a particular case."

The comments of Gates, who has the closest relations with the White House, echoed those of FBI Director James Comey, who wrote over the weekend that "the San Bernardino litigation isn't about trying to set a precedent or send any kind of message."

In fact, this is precisely the administration's intention.

The context of the present case is a concerted effort by the political establishment and the media to counter the wave of popular anger that followed the revelations by Edward Snowden, beginning in the summer of 2013, of illegal and unconstitutional spying by the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI). Snowden exposed programs that accumulate vast databases of information, including telephone records, emails, Internet traffic and anything else that can reveal the political activity and relations of anyone, anywhere in the world. In part in response to these revelations, security measures to prevent government snooping have become more popular and more widely accessible.

Last year, Congress began preparing legislation to require technology companies to install "backdoors" that would allow the government access to encrypted data on demand. The White House decided in the fall not to press forward with the bill. Citing senior administration officials, the *Washington Post* noted at the time that the decision was motivated, in part, by an effort to "repair global trust in the US government and US tech companies, whose public images have taken a beating" in the wake of the Snowden revelations.

While continuing to warn about encryption (what Comey called "going dark"), the White House waited for better conditions to press forward. Behind the scenes, it was quite explicit about how it intended to push its spying agenda. Robert Litt, the top lawyer for the Office of the Director of National Intelligence, wrote in one email obtained by the *Post* that "the legislative environment… could turn in the event of a terrorist attack or criminal event." The intelligence agencies should be "keeping our options open for such a situation."

An unnamed senior administration official complained to the *Post* that "we do not have the perfect example where you have the dead child or a terrorist act to point to, and that's what people seem to claim you have to have."

The San Bernardino killings, which left 14 people dead, provided the desired "perfect example." Immediately, the demand was raised by CIA Director John Brennan, Comey and other intelligence officials for legislation to force companies to provide a backdoor to encryption. The FBI, with the backing of the White House, decided to make the case against Apple a public

battle for this purpose. The legislation shelved last year is being revived in Congress.

The specific powers the government is seeking in the court case are themselves extremely far-reaching. Data on more recent iPhones is encrypted and protected by a password or passphrase. The phone has an additional security feature that deletes all data if too many incorrect passwords are entered, preventing the government from using a "brute force" technique of entering every possible combination.

These smartphones contain an immense amount of personal information, including lists of contacts, emails and texts, phone records, photographs, historical data on physical movements, private PGP keys for encrypted emails, bank account data and much more.

The government is seeking to require Apple to write and install a new version of its operating system to override the phone's security features. If the government succeeds, it will give it the power to use the same procedure on any other phone it wants to access.

Even more significantly, a precedent will be established to require any company to do something similar: create and program backdoors to allow government access to encrypted communications. This overrides the basic purpose of encryption, which is precisely what the administration is seeking to do.

These efforts are a continuation of the policy of the American ruling class since the beginning of the "war on terror," now in its 15th year. Democratic rights—including the Fourth Amendment safeguards against unreasonable searches and seizures—have been under relentless assault under cover of a phony crusade against terrorism. First Bush and then Obama have overseen an immense expansion of state powers to spy on the population.

In doing so, the government has worked closely with the gigantic companies that control the communication networks, a fact that is underscored by Gates' intervention in the dispute between the government and Apple. For its part, Apple is motivated not by principled considerations, but by business interests. It has its own ties with intelligence agencies and has made clear that it would have been willing to work out some sort of arrangement behind the scenes if the administration had not decided to make its demands public.

Within the political establishment, there is uniform support for the destruction of democratic rights. It is notable that, alongside the war plans of the American ruling class, domestic spying is a non-issue in the presidential election campaign.

When it has come up, the various candidates have backed the intelligence agencies. Bernie Sanders, when asked in a debate earlier this month about his position on the Apple case, said that he supported both sides. Accepting the framework of the "war on terror," Sanders said that he "worries about the possibility of another terrorist attack against our country." He hoped that Apple and the government could find a "middle ground."

This is consistent with Sanders' call for the prosecution of Snowden.

Terrorism is being used as a pretext. The expansion of state powers is aimed fundamentally at the working class.

Presiding over a social system riven by extreme levels of social inequality, and anticipating growing anger over its policies of war and social reaction, the financial aristocracy is preparing accordingly. It is on the working class, organized as an independent force in opposition to the entire capitalist system, that the defense of democratic rights must be based.