US Attorney General Barr demands law enforcement “backdoor” access to encrypted data and communications

By Kevin Reed
26 July 2019

In a significant escalation of the US government’s assault on democratic rights, Attorney General William Barr gave a speech on Tuesday in which he asserted that tech companies “can and must” provide law enforcement agencies with backdoor access to encryption on electronic devices and software applications used widely by people all over the world.

Speaking before an audience of law enforcement officials, Barr expressed the contempt of the entire state apparatus for the public by saying the security risks of backdoor access should be accepted because “after all, we are not talking about protecting the Nation’s nuclear codes.”

Delivering his speech at the Eighth International Conference on Cyber Security in New York City hosted jointly by the Federal Bureau of Investigation (FBI) and Fordham University, Barr said the refusal of “service providers, device manufacturers and application developers” to allow police agencies access to encrypted data “poses a grave threat to public safety.”

Barr referred to the current widely implemented data encryption methods as “warrant-proof” because “even with a warrant based on probable cause” police are “prevented from accessing communications in transit or data stored on cell phones or computers.” He said this type of encryption is “extinguishing the ability of law enforcement to obtain evidence.”

Of course, the attorney general argued that police needed access to encrypted data in order to stop “violent criminals, terrorists, drug traffickers, human traffickers, fraudsters and sexual predators” from operating “with impunity, hiding their activities under an impenetrable cloak of secrecy” by “going dark.”

Encryption methods have been deployed aggressively by the giant Silicon Valley tech firms like Microsoft, Google, Apple and Facebook in the years following the revelations of former intelligence officer Edward Snowden that the National Security Agency (NSA) was conducting a massive and illegal operation to collect and store the digital communications of the entire population of the world.

Through arrangements with the telecom corporations, the NSA has been tapping into the international communications trunk lines and satellites and the backbone of the internet to gather the content of data transmissions, email and telephone calls and storing them in massive secret data centers in remote locations in the US. The subsequent proliferation of strong encryption techniques has put a significant dent in this surveillance operation.

Given this reality, it is entirely reasonable for the public to demand that their computers and smartphones be equipped with encryption that prevents the national security state from violating their basic democratic rights. And clearly, Barr’s “crime fighting” arguments in favor of cracking encryption are entirely hypocritical since the number one organization operating internationally “with impunity, hiding their activities under an impenetrable cloak of secrecy” is the US government itself.

Data encryption on most consumer electronic devices like smartphones and computers has two forms. The first involves the transmission of electronic or voice and video communications between devices. The most common method used is called End-to-End Encryption (E2EE) where only the users of the information on the sending and receiving ends can read, hear or watch the communications.

The E2EE system prevents electronic surveillance—by the government and telecom and internet companies—from being able to intercept and decipher the communications. With the use of public and private cryptographic keys, correspondents exchange communications intended only for each other. The decryption of the messages can only be accomplished with the appropriate public and private key combinations.

E2EE communications are increasingly being used by smartphone texting apps and voice and video computer communications tools where the “keys” are embedded in the software and encryption is always active. Among the most commonly used smartphone apps that employ E2EE encryption by default are WhatsApp, Signal and WickrMe.

The second kind of encryption concerns the data stored on a device. This encryption involves scrambling the data on the computer, smartphone or tablet such that an invasive action like tethering the device to another computer or removing the storage drive or memory chips cannot allow access to the data by anyone other than the user.

Most smartphones and tablets feature data encryption by default once a PIN (personal identification number) or biometric access such as a Touch ID or Face ID has been set on the device. Some devices require a second step to initialize encryption separately from setting the PIN. The data on Apple iPhones, iPads and Android-based smartphones and tablets are encrypted by default.

Personal computers typically require an additional step to encrypt the contents of the storage drive. This is true for MacOS and Windows PCs, and also requires setting up of security passwords.

Backdoor access means that a special key can be applied to encrypted communications in transit or encrypted data-at-rest enabling a third-party or government agency to read or view the data contents. Most technology experts have responded to the idea of backdoor access by the police as "a terrible idea." Tech experts have consistently argued that backdoors will put millions of people at risk because the special keys created for law enforcement will inevitably be stolen or hacked from the authorities entrusted to protect them.

Barr's speech follows by one month a meeting of senior Trump administration officials—the National Security Council Deputies Committee—which was devoted to the topic of encryption. At that time, a leaked media report revealed that the discussion revolved around whether or not to push for Congressional legislation to make E2EE and device encryption without backdoor access illegal.

Indicating that the Trump administration is now planning to force the issue into the courts, Attorney General Barr went into a lengthy legal argument to justifying the demand for backdoor access. In discussing the Fourth Amendment—which explicitly upholds the right of individuals against unreasonable searches and seizures by the government—Barr said, "our societal response to advances in technology that affect the balance between individual privacy and public safety has been—and always should be—a two-way street."

He then went on to say, "given the frequency with which these situations are now arising, it is only a matter of time before a sensational case crystalizes the issue for the public." In other words, the US Justice Department is in the hunt for a test case in US courts that will bring a ruling that achieves their objective.

Barr also went into the international imperialist collaboration underway with the GCHQ in Britain in devising invasive technical approaches to backdoor access. Something called "Virtual Alligator Clips" has been developed that would allow a technology provider to "respond to a warrant by adding a silent law enforcement recipient to an otherwise secure chat." Another solution called "Layered Cryptographic Envelopes" would "allow lawful access to encrypted data-at-rest on disks or other storage devices."

Barr acknowledged that there were "putative shortcomings" to these ideas and urged further "refinements and alternative proposals" and offered that "through this dialectic we can identify workable solutions." In other words, despite his high-sounding language, the DOJ has no solid technical proposals and is, instead, attempting to strong-arm the tech industry into providing its own solution.

The conflict between federal law enforcement and the tech companies over encryption has been going on for several years. When the FBI—then under the direction of James Comey—demanded in December 2015 that Apple provide backdoor access to the iPhone of one of the San Bernardino terrorists, the company refused. The FBI and DOJ then threatened the unprecedented use of the All Writs Act of 1789 to force Apple to help crack open the phone contents.

On February 16, 2016, Apple published a letter to customers where it explained its stance: "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."

Of course, no one should accept the claims of the DOJ that the purpose of the drive to break encrypted data is about fighting crime. As was shown by the June 26 meeting at the White House, the entire military-intelligence state apparatus is working on this issue as a matter of national security.

The speech by William Barr should be understood by workers internationally—particularly those in the tech industry—as a threat and significant escalation of the assault on basic democratic by the US government. Within the context of the drive by the Trump administration toward authoritarian forms of rule and Trump's fascistic denunciations of socialism—with the support of the Democratic Party—the working class must be aware of the preparations for a police state that are contained in the demand that the tech industry allow backdoor access to encryption.

Up to this point, the position of Apple has been shared consistently by the majority of the tech industry, except for those with close ties to the state. The giant consumer technology companies—mainly for business reasons and concerns about potential loss of global market share—have not yet compromised on the principle that one single backdoor key to encryption will break the entire system. However, if the DOJ is successful in getting a court ruling that makes strong encryption on consumer electronics devices illegal, it is entirely likely that—especially if such a ruling includes the imposition of significant financial penalties for non-compliance—that the tech companies will reverse their position.