FBI using hacker techniques to spy on Americans

Thomas Gaist
5 August 2013

In yet another revelation of illegal spying on Americans by the US government, reports last week detailed the use by the Federal Bureau of Investigation (FBI) of hacker techniques, including spyware, to gain access to information protected by encryption tools and other communications technologies. In law enforcement terminology, use of such technology to secure communications against interception is known as "going dark."

The FBI has been building teams of hackers and arming them with cyber-weapons. Unnamed former officials told the *Wall Street Journal* ["FBI Taps Hacker Tactics to Spy on Suspects," August 3] that the FBI's hacking activities are led by a group called the Remote Operations Unit. According to a former FBI cyber division official, the bureau "hires people who have hacking skill, and they purchase tools that are capable of doing these things."

Hacking techniques enable the FBI to smuggle spyware into computers and laptops. The *Journal* reported that the FBI has been using "web bugs" since at least 2005 to extract data from targeted computers. According to a US official cited by the *Journal*, the FBI is even able to activate microphones in telephones using Google Inc.'s Android software.

The FBI has sought to conceal these activities from the public. As a US official commented to the *Journal*, the bureau "is loath to use these tools when investigating hackers," fearing that computer savvy targets will figure out what is going on and report the use of hacker methods to the public.

Christopher Soghoian, a technology expert at the American Civil Liberties Union, said that awareness of use of such techniques by law enforcement is growing as a result of an emerging industry based on selling hacking tools to government agencies. "People should understand that local cops are going to be hacking into surveillance targets," said Soghoian.

These revelations are only the latest in an ongoing cascade of exposures of a pervasive police state system of surveillance operating every day in the US. Numerous US government operations are now known to involve mass data mining without specific warrants, including: the seizure of telephone metadata, the PRISM program for intercepting email and other Internet communications, the recording of license plates, the photographing of mail, the tracking of cell phone communications, and the XKeyscore program, which allows the NSA to carry out everything from dragnet surveillance to the reading of the contents of individual emails.

Repeated claims by President Obama, intelligence officials and lawmakers as to the supposedly legal and narrowly targeted character of these programs have been exposed as lies. All of these surveillance programs violate the Fourth Amendment to the US Constitution, which bans unreasonable searches and seizures and stipulates the need for specific court-issued warrants.

"What I can say unequivocally is that if you are a US person, the NSA cannot listen to your telephone calls, and the NSA cannot target your emails… and have not," Obama told PBS Television during an interview in mid-July.

These words stand in flat contradiction to facts that are now a matter of public record. Extended warrants for mass data collection and surveillance are regularly approved by the secret Foreign Intelligence Surveillance (FISA) court, which has rejected only 11 surveillance requests out of nearly 34,000 submitted. On the basis of these secret authorizations, US law enforcement and intelligence agencies operate an information gathering machinery which spans the entire

globe and can assemble detailed personal and political profiles on anyone who uses the internet or a telephone.

A number of Democratic lawmakers, such as senators Ron Wyden and Mark Udall, have presented themselves as opponents of the surveillance programs. They are leading a group of legislators who are proposing measures that would, they claim, "fundamentally reform" surveillance policy.

Such claims are deliberately deceptive. The steps being proposed by Wyden and Udall would place modest restrictions on the unconstitutional programs, while allowing them to continue in violation of basic privacy and democratic rights. They also include loopholes and caveats that would enable the NSA, FBI and other agencies to use "national security" as a pretext for ignoring even the minor restraints they are proposing. In essence, the "reforms" proposed by this group are aimed at providing a fig leaf of legality and "transparency" on illegal government surveillance of the American people.

Congress and both political parties were fully informed about the programs from the beginning and gave their approval.

The most "radical" of the reform proposals is that of House Democrat Rush Holt, who has proposed to repeal the USA Patriot Act of 2001 and the FISA Amendments Act of 2008. Holt implied in recent remarks that claims by top officials that the surveillance programs stopped over 50 terrorist attacks were untrue, saying: "I learned that the heads of the NSA and other intelligence agencies are schooled in secrecy and deception."

Yet neither Holt nor any of the other congressional critics propose impeaching the responsible officials—from Obama and the head of the NSA, CIA and FBI on down—and prosecuting them for crimes against the US Constitution that go far beyond anything carried out by Richard Nixon.

There is no reform solution to the growth of police state powers. They are embedded in the capitalist system and the massive growth of social inequality and militarism that it engenders. The ruling class is building up the structure of a police state because it anticipates the growth of social opposition to its policies of austerity at home and war abroad, and is preparing to meet this threat with state violence and repression.

It is necessary to dismantle the military-intelligence apparatus and end the rule of the banks and corporations that it upholds, as part of an international struggle of the working class for socialism.