GlobalResearch
Center for Research on Globalization

Domestic Spying and Social Media: Google, Facebook “Back Doors” for Government Wiretaps

By Andre Damon
Global Research, May 09, 2013
World Socialist Web Site

Region: USA
Theme: Police State & Civil Rights

The Obama administration is close to announcing its support for a law that would force Google, Facebook and other Internet communications companies to build back doors for government wiretaps, according to an article in the New York Times Wednesday.

Such a measure would allow intelligence agencies, particularly the FBI, to monitor a vast array of communications, including Facebook messages, chats, and email using services such as Gmail.

The move comes as the National Security Agency’s sprawling new data center in Utah prepares to come online in September of this year. The facility is rumored to store data on the scale of trillions of terabytes, meaning that it can easily house the contents of every personal computer in the world.

Under the terms of the 1994 Communications Assistance for Law Enforcement Act, known as CALEA, hardware used to facilitate Internet and voice communications—the networks through which data is transmitted—must have the technical means to allow the government to conduct wiretaps.

The spying capabilities created in the context of this earlier law made possible the massive illegal domestic spying programs conducted under the Bush administration, and tens of thousands of ongoing secret court-approved wiretaps conducted under Obama. Under Bush, reports emerged that the government was essentially given full access to transmission systems by many Internet Service Providers (ISPs), such as AT&T.

US intelligence agencies were satisfied with these capabilities up until around 2010, when, in response to a series of security breaches, services such as Gmail and Facebook enabled encryption by default.

As a result of this move, communications using these services became inaccessible to conventional wiretapping, which relied on intercepting the (now encrypted) data traveling between users and routed by ISPs.

To offset the effects of encryption, the FBI has sought to force companies to create back doors for surveillance, with varying degrees of success. Following its purchase by Microsoft, Skype, the online chat and voice service, last year voluntarily reengineered its architecture to allow the US and other governments to monitor chat communications.

The FBI claims that, under current laws, Internet communications companies can effectively

refuse to comply with a court-ordered wiretap by claiming that there is no practical way for them to allow the government to spy on their users' communications.

The proposed law would force social networks and other communications companies to provide government access or face fines that, according to the *Washington Post,* would multiply exponentially and threaten companies with bankruptcy.

While keeping silent on the unconstitutional nature of the US government's vast domestic spying apparatus, groups representing major Silicon Valley corporations have raised concerns about the difficulty of implementing the proposed government wiretapping capabilities, particularly for start-ups and small companies, which behemoths like Facebook and Apple rely on for developing new technologies.

According to the *Times*, officials are working to reformulate the law to satisfy these concerns while forcing the most widely used services to allow wiretapping.

"While the F.B.I.'s original proposal would have required Internet communications services to each build in a wiretapping capacity, the revised one, which must now be reviewed by the White House, focuses on fining companies that do not comply with wiretap orders," the *Times* reported. "The difference, officials say, means that start-ups with a small number of users would have fewer worries about wiretapping issues unless the companies became popular enough to come to the Justice Department's attention."

In addition to forcing Internet communications companies to allow wiretapping, the law would also put even more pressure on ISPs to ensure that they do not break the government's existing wiretapping capabilities by upgrading their systems.

The Obama administration's drive to expand the government's wiretapping comes in the aftermath of the Boston Marathon bombings, which have been used as the pretext for the implementation of a range of police state measures, including most notably the lockdown of Boston following the blasts.

The Obama administration has claimed that its wiretapping activities are conducted under warrants issued by a FISA court, which essentially rubber-stamp government spying applications. In 2012, the FISA court did not deny a single application for spying.

However, the full extent of the government's wiretapping programs is kept totally secret, and its real scope is far more sweeping than what has already been admitted.

A hint of the potentially vast extent of domestic spying was indicated by Tim Clemente, a former FBI counterterrorism agent, last week, in an interview with CNN's Erin Burnett. Burnett asked Clemente if there was any way that the government would be able to implicate the widow of Boston Marathon bombing suspect Tamerlan Tsarnaev in playing a role in the bombing.

Clemente responded by saying, "We certainly have ways in national security investigations to find out exactly what was said in that [phone] conversation. It's not necessarily something that the FBI is going to want to present in court, but it may help lead the investigation and/or lead to questioning of her."

By stating that the evidence would not be admissible in court, Clemente was implying that the evidence was gathered illegally. Faced with skepticism from Burnett about the

government's ability to access such data, Clemente added, "Welcome to America. All of that stuff is being captured as we speak whether we know it or like it or not."
