Obama seeks Silicon Valley aid to spy on social media

Thomas Gaist
9 January 2016

White House officials met with Silicon Valley executives Friday to discuss the US government's expanding efforts to monitor and intervene in online social media and other forms of internet communication.

The meeting, held in San Jose, California, featured high-level figures from Silicon Valley, including Apple CEO Tim Cook, and a government delegation led by White House Chief of Staff Denis McDonough, Attorney General Loretta Lynch, Director of National Intelligence James Clapper, NSA Director Michael Rogers and FBI Director James Comey.

According to an official statement issued by the White House, the purpose of the meetings was to "work together to combat terrorism and counter violent extremism online."

During the tech summit, the White House delegation circulated proposals calling for tech firms to develop tools to "measure radicalization" levels among different populations, and to enable more effective dissemination of government-produced anti-terrorist media, documents acquired and published by The Intercept on Friday show.

Also on Friday, with the closed-door discussions still in progress, the White House announced new programs against "violent extremism" in the United States, including the establishment of a new Countering Violent Extremism task force, to be formed jointly by the Department of Homeland Security and the Department of Justice.

The new CVE task force, based out of DHS facilities, will seek to "integrate and harmonize" the operations of "dozens of federal and local agencies," according to unnamed US officials cited by the Washington Post. The newly formed DHS-led task force will "coordinate all of the government's domestic counter-radicalization efforts," according to the US officials who spoke to the Post.

The State Department will also create a new Global Engagement Center to coordinate US government social media work internationally, a White House statement said.

Friday's high-profile Silicon Valley summit and the announcement of the new counterterror programs have confirmed that the Obama administration will make use of its final year in power to further entrench and expand the surveillance apparatus.

The Obama administration aims to spend 2016 "overhauling its propaganda war against the Islamic State," the Washington Post reported Thursday, in an article based on leaks from unnamed, high-level US government sources.

New spy programs launched by the administration will seek to collect and analyze data from social media networks and develop covert operations that allow the government to use the networks for its own counter-radicalization schemes, the US officials said.

The Obama White House has already overseen the development of a raft of police-state measures in the name of fighting "violent extremism," hosting two major international conferences last year as part of efforts to coordinate surveillance projects among the various imperialist powers.

As early as 2012, the US government began seeking private contractors to conduct surveillance and analysis of social media data on behalf of the agency, through which the bureau could "develop pattern of life matrices" to enable law enforcement agencies to automatically identify likely "radicals."

Recent months have seen growing clamor by the American state against encryption technology, as FBI Director James Comey has staged numerous public

appearances to demand that the US government be given unlimited "back door" access to all encryption systems used by US communications firms.

The US political and media establishments have sought to justify this agenda by lamenting the limitations of previous social media surveillance efforts, endlessly repeating claims—without any factual basis—that the attacks in San Bernardino and elsewhere could have been stopped through preemptive screening of social media profiles for signs of extremism.

A growing stream of reports from elite universities and US government agencies warn—again without any evidence—that the Internet is enabling mass conversions of US residents into violent terrorists. Media reports this week highlighted one recent contribution, ludicrously titled "ISIS in America: From Retweets to Raqqa," published in December 2015 by George Washington University's "Program on Extremism."

In the period since the exposure by NSA contractor Edward Snowden of massive US government spying on the Internet, many Silicon Valley firms have sought to pose as defenders of privacy against government overreach, although they have cooperated extensively with the government's surveillance operations for years.

The communications firms are mainly concerned to protect the illusion of independence from the government, rather than to actually protect the privacy of their users, as comments by an unnamed Silicon Valley official reported by the Washington Post on Friday made clear. "Being seen as having the US government force our hands makes others around the world lose confidence in us," an unnamed Silicon Valley official told the newspaper.

Friday's meeting, with its lineup of virtually every top US official overseeing counterterrorism and surveillance, demonstrates that the US ruling elite is seeking nothing less than to subject the entire world communications system to unlimited scrutiny by US security and intelligence agencies.

Whether or not the leading tech companies will sign on to the specific initiatives being put forward by the White House Friday remains unclear. Nonetheless, as revelations from Snowden have conclusively shown, all the major communications providers have collaborated to varying degrees with the illegal mass spying operations erected by the US government since 9/11.

The events of the past decade-and-a-half have made clear that the entire corporate and political establishment favors an agenda of police-state spying on the American population.

In the immediate aftermath of 9/11, AT&T allowed the CIA and NSA continuous direct access to the company's servers via special rooms installed inside the corporation's headquarters.

The NSA has enjoyed virtually unfettered access to the servers of major Internet and telephone providers for years as part of secret deals negotiated in connection with the agency's PRISM program. Since 2007, the US government has successfully recruited Microsoft, Google, Facebook, YouTube, AOL, Skype and Apple as participants in PRISM, giving the NSA complete access to all live communications hosted on the corporate servers, including email, video and voice calls, chats and file exchanges, along with unlimited access to their data archives.

Terrified by the Snowden exposures, the US government has increasingly turned these methods on its own employees, who are now among the most heavily surveilled groups on the planet. As part of the Pentagon-led "Insider Threat Program," at least 100,000 US government employees have been targeted by highly intrusive electronic surveillance, a 2015 Congressional report secured in December by a Freedom of Information Act request revealed.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact