

The intelligence-industrial complex

Joseph Kishore
15 July 2013

An important aspect of the spying operations that have been exposed over the past month by National Security Agency (NSA) whistle-blower Edward Snowden is the collusion of giant telecommunications and technology companies with the Obama administration and US intelligence agencies in the systematic violation of democratic rights.

A major element in this corporate-intelligence nexus was revealed late last week in articles detailing software giant Microsoft's intimate relations with the NSA and the FBI.

According to Snowden, Microsoft worked with the NSA to develop procedures to get around the company's own encryption mechanisms, allowing unfettered access to its Outlook.com service, which includes Hotmail, Messenger and other widely used programs. It also collaborated with the FBI and NSA to ensure access to SkyDrive, a file-hosting service used by some 250 million people.

In 2011, Microsoft acquired Skype, a chat, voice and video communications system that currently has 800 million users. While Skype had already begun collaborating with US spy agencies, the NSA boasted that nine months after Microsoft took over the company, the number of video calls accessed by the agency had tripled.

The US government's relations with Microsoft are critical to its efforts to accumulate databases containing vast stores of information. Microsoft is the world's largest software maker, run by the world's second-wealthiest individual, Bill Gates. The company's Windows operating system is used on nearly 90 percent of web-connected computers. Given the latest revelations, it should be assumed that most actions performed on Microsoft computers are susceptible to government monitoring.

Microsoft is by no means the only company working secretly, behind the backs of its customers, to provide

massive amounts of information to the state.

The first revelation by Snowden concerned an order from the Foreign Intelligence Surveillance Court requiring telecommunications giant Verizon to turn over the phone records of its millions of customers. This is part of a program, begun in 2006 and continued under Obama, to collect "metadata" from all the major phone companies, including AT&T and Sprint. With detailed information on who called whom, when, and from where, the state is able to determine the social and political relations of virtually every resident of the United States.

The spying on Skype users is part of the broader PRISM program, begun in 2007, through which the NSA has gained direct access to the servers of US Internet companies, including Microsoft, Yahoo, Google, Facebook, AOL, YouTube and Apple.

PRISM itself is only part of an even more expansive program, in which the NSA taps directly into the "Internet backbone"—the system of fiber optic cables through which most telecommunications and Internet communications pass. These cables are run and controlled by large corporations, including the same telecommunications giants that hand over data on phone records, as well as companies such as 3 Communications and CenturyLink. In this way, the NSA can monitor in real time much of the world's Internet traffic and reroute it for permanent storage.

Bloomberg News reported last month that "thousands of technology, finance and manufacturing companies are working closely with US national security agencies, providing sensitive information and in return receiving benefits that include access to classified information." In exchange for their secret collaboration with the government, the companies often receive documents guaranteeing immunity for their actions.

The programs cited by Bloomberg are diverse and far-reaching. They include an agreement with Microsoft to

inform the NSA of bugs in its operating systems before they are publicly released—giving the agency an opportunity to exploit the information to infiltrate computers in the US and abroad. McAfee, which makes Internet security software and is a subsidiary of Intel, also partners with intelligence agencies on a regular basis.

The corporate-intelligence collaboration is global. Over the weekend, newspapers in Australia reported on a partnership between US spy agencies and Telstra, the largest telecommunications company in Australia, to hand over data to the US government. Telstra controls the bulk of the Internet backbone in Australia and routes much of the communications traffic from Asia.

Earlier this month, Glenn Greenwald, the journalist who has worked with Snowden, reported in the Brazilian newspaper *O Globo* of a program, dubbed FAIRVIEW, that has collected billions of communications of ordinary Brazilians. Again, telecommunications companies have been directly involved. According to Greenwald, “the NSA partners with a large US telecommunications company... and that US company then partners with telecoms in foreign countries.” The foreign telecoms provide data to the US company, which delivers it to the NSA.

In some cases, the intimate connection between intelligence agencies and telecommunications companies involves the passage of individuals directly from one to the other. For example, the current chief of security for Verizon, Michael Mason, is the former chief of the FBI’s Criminal, Cyber, Response and Services Branch. The same position at AT&T is held by Edward Amoroso, a member of President Reagan’s “Strategic Defense Initiative” in the 1980s—the project to build a missile defense shield over the US.

In 1961, in his farewell address, US President Dwight Eisenhower warned of the “military-industrial complex,” which he described as “the conjunction of an immense military establishment and a large arms industry.” This growing nexus posed the threat of the “disastrous rise of misplaced power,” which, he declared, “endangers our liberties and democratic processes.”

Fifty years later, the integration of the military-intelligence apparatus and giant corporations is far more advanced than anything Eisenhower could have imagined. Not only does the military have the closest

relations with private contractors for the production of weapons, but the state, acting on behalf of the ruling class as a whole, has developed a network of relations with gigantic corporations to spy on the population.

As the *World Socialist Web Site* has repeatedly insisted, democratic rights are not compatible with the continued rule of the corporate-financial elite and the capitalist system upon which it rests. The American ruling class is carrying out a global policy of war and social counter-revolution. The construction of a police state apparatus is aimed above all at the working class and will be used against social and political opposition to this policy.

The exposure of the intelligence-industrial complex makes clear that the defense of democratic rights is inextricably tied to the fight for the democratization of economic life and socialism. Critical social infrastructure, including telecommunications, must be taken out of the hands of private companies and placed under the democratic control of the working class. Corporations such as Microsoft, Apple, Verizon and AT&T, and their counterparts internationally, must be transformed into publicly-owned utilities, run on the basis of social need, not private profit.



To contact the WSWS and the
Socialist Equality Party visit:

wsws.org/contact