GlobalResearch
Center for Research on Globalization

# Government Spying on Americans … and then Giving Info to Giant Corporations

## Big Banks and Other Corporate Bigwigs Benefit from Illegal Spying

By Washington's Blog
Global Research, June 12, 2013
Washington's Blog

Region: USA
Theme: Global Economy, Intelligence, Police State & Civil Rights

You've heard that the government spies on all Americans.

But you might not know that the government shares some of that information with big corporations.

In addition, Reuters reported in 2011 that the NSA shares intelligence with Wall Street banks in the name of "battling hackers."

> The National Security Agency, a secretive arm of the U.S. military, has begun providing Wall Street banks with intelligence on foreign hackers, a sign of growing U.S. fears of financial sabotage.The assistance from the agency that conducts electronic spying overseas is part of an effort by American banks and other financial firms to get help from the U.S. military and private defense contractors to fend off cyber attacks, according to interviews with U.S. officials, security experts and defense industry executives.
>
> The Federal Bureau of Investigation has also warned banks of particular threats amid concerns that hackers could potentially exploit security vulnerabilities to wreak havoc across global markets and cause economic mayhem.
>
> ***
>
> NSA Director Keith Alexander, who runs the U.S. military's cyber operations, told Reuters the agency is currently talking to financial firms about sharing electronic information on malicious software, possibly by expanding a pilot program through which it offers similar data to the defense industry.
>
> ***
>
> NSA, which has long been charged with protecting classified government networks from attack, is already working with Nasdaq to beef up its defenses after hackers infiltrated its computer systems last year and installed malicious software that allowed them to spy on the directors of publicly held companies.
>
> ***
>
> The NSA's work with Wall Street marks a milestone in the agency's efforts to make its cyber intelligence available more broadly to the private sector.
>
> ***
>
> Greater cooperation with industry became possible after a deal reached a year

> ago between the Pentagon and the Department of Homeland Security, allowing NSA to provide cyber expertise to other government agencies and certain private companies.

In March, PC Magazine noted:

> "Right now, the ability to share real-time information is complicated and there are legal barriers. We have to overcome that," Gen Keith B. Alexander, director of the National Security Agency and commander of U.S. Cyber Command, said during a Thursday appearance at Georgia Tech's Cyber Security Symposium.
>
> [Alexander has been pushing for the anti-privacy Internet bill known as "CISPA" to be passed.] "It allows the government to start working with industry and … discuss with each of these sector about the best approach," he said.

CISPA would allow the NSA to more openly share data with corporations in the name of protecting against "cyber threats." But that phrase is too squisy. As the Electronic Frontier Foundation notes:

> A "cybersecurity purpose" only means that a company has to think that a user is trying to harm its network. What does that mean, exactly? The definition is broad and vague. The definition allows purposes such as guarding against "improper" information modification, ensuring "timely" access to information or "preserving authorized restrictions on access…protecting…proprietary information" (i.e. DRM).

Moreover, as the ACLU notes, "Fusion Centers" – a hybrid of military, intelligence agency, police and private corporations set up in centers throughout the country, and run by the Department of Justice and Department of Homeland Security – allow big businesses like Boeing to get access to classified information which gives them an *unfair advantage* over smaller competitors:

> Participation in fusion centers might give Boeing access to the trade secrets or security vulnerabilities of competing companies, or might give it an advantage in competing for government contracts. Expecting a Boeing analyst to distinguish between information that represents a security risk to Boeing and information that represents a business risk may be too much to ask.

A 2008 Department of Homeland Security Privacy Office review of fusion centers concluded that they presented risks to privacy because of ambiguous lines of authority, rules and oversight, the participation of the military and *private sector*, data mining, excessive secrecy, inaccurate or incomplete information and the dangers of mission creep.

The Senate Permanent Subcommittee on Investigations found in 2012 that fusion centers spy on citizens, produce 'shoddy' work unrelated to terrorism or real threats:

> "The Subcommittee investigation found that DHS-assigned detailees to the fusion centers forwarded 'intelligence' of uneven quality – oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."

Under the FBI's Infraguard program, businesses sometimes receive intel even *before* elected officials.

Law enforcement agencies spy on protesters and then share the info – at taxpayer expense – with the giant Wall Street banks

And a security expert says that all Occupy Wall Street protesters had their cellphone information logged by the government.

Alternet notes:

> Ironically, records indicate that corporate entities engaged in such public-private intelligence sharing partnerships were often the very same corporate entities criticized, and protested against, by the Occupy Wall Street movement as having undue influence in the functions of public government.

In essence, big banks and giant corporations are seen as being part of "critical infrastructure" and "key resources" ... so the government protects them. That creates a dynamic where the government will do quite a bit to protect the big boys against any real or imagined threats ... whether from activists or even smaller competitors. (Remember that the government has completely propped up the big banks, even though they went bankrupt due to stupid gambles.)

And given that some millions of private contractors have clearance to view information gathered by spy agencies, and that information gained by the NSA by spying on Americans is being shared with agencies in other countries, at least some of the confidential information is undoubtedly leaking into private hands *even without* the government's knowledge or consent.

As the ACLU noted in 2004:

> There is a long and unfortunate history of cooperation between government security agencies and powerful corporations to deprive individuals of their privacy and other civil liberties, and any program that institutionalizes close, secretive ties between such organizations raises serious questions about the scope of its activities, now and in the future.

Indeed, the government has been affirmatively helping the big banks, giant oil companies and other large corporations cover up fraud and to go after critics. For example, Business Week reported on May 23, 2006:

> President George W. Bush has bestowed on his intelligence czar, John Negroponte, broad authority, in the name of national security, to excuse publicly traded companies from their usual accounting and securities-disclosure obligations.

Reuters noted in 2010:

> U.S. securities regulators originally treated the New York Federal Reserve's bid to keep secret many of the details of the American International Group bailout like a request to protect matters of national security, according to emails obtained by Reuters.

Wired reported the same year:

> The DHS issued a directive to employees in July 2009 requiring a wide range of public records requests to pass through political appointees for vetting. These included any requests dealing with a "controversial or sensitive subject" or pertaining to meetings involving prominent business leaders and elected officials. Requests from lawmakers, journalists, and activist and watchdog groups were also placed under this scrutiny.

In an effort to protect Bank of America from the threatened Wikileaks expose of wrongdoing – the Department of Justice told Bank of America to a hire a specific hardball-playing law firm to assemble a team to take down WikiLeaks (and see this)

The government and big banks actually coordinated on the violent crackdown of the anti-big bank Occupy protest.

The government is also using anti-terrorism laws to keep people from learning what pollutants are in their own community, in order to protect the fracking, coal and other polluting industries. See this, this, this, this and this.

Investigating factory farming can get one labeled a terrorist.

Infringing the copyright of a big corporation may also get labeled as a terrorist … and a swat team may be deployed to your house. See this, this, this and this. As the executive director of the Information Society Project at Yale Law School notes:

> This administration … publishes a newsletter about its efforts with language that compares copyright infringement to terrorism.

In short, the "national security" apparatus has been hijacked to serve the needs of big business



---

*Articles by:* Washington's Blog