

# Former CIA Employee Snowden, Blows Whistle on NSA's Dragnet Surveillance

By [Prof. Marjorie Cohn](#)

Global Research, June 12, 2013

[Truthout](#)

Region: [USA](#)

Theme: [Intelligence](#), [Police State & Civil Rights](#)

Just as Bradley Manning's court-martial was getting underway, another brave whistleblower dropped a bombshell into the media: The Obama administration is collecting data on every telephone call we make. Nearly 64 years to the day after George Orwell published his prescient book 1984, we have learned that the "Thought Police" are indeed watching every one of us. "They quite literally can watch your ideas form as you type," Edward Snowden told the Washington Post.

A former undercover CIA employee who has worked at the National Security Agency (NSA) for four years, Snowden provided a secret order of the Foreign Intelligence Surveillance Court to the Guardian. The order requires Verizon on an "ongoing daily basis" to provide the NSA information about all phone calls in its system both in the United States and other countries. Glenn Greenwald wrote that it "shows for the first time that under the Obama administration the communication records of millions of U.S. citizens are being collected indiscriminately and in bulk – regardless of whether they are suspected of any wrongdoing." That secret order is scheduled for declassification on April 12, 2038.

The order, issued under Section 215 of the Patriot Act, mandates that Verizon provide daily phone records for all "communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." The government is collecting "metadata" on our phone communications. That is, the identities of the sender and recipient, and the date, time, duration, place, and unique identifiers of the communication. Administration officials defending the program claim they are not reading the content of our calls.

But, as ACLU's Ben Wizner and Jay Stanley note, "Even without intercepting the content of communications, the government can use metadata to learn our most intimate secrets – anything from whether we have a drinking problem to whether we're gay or straight ... The 'who,' 'when' and 'how frequently' of communications are often more revealing than what is said or written." For example, "Repeated calls to Alcoholics Anonymous, hotlines for gay teens, abortion clinics or a gambling bookie may tell you all you need to know about a person's problem." And, they add, "URLs often contain content – such as search terms embedded within them," so that "the very fact that we've visited a page with a URL such as '[www.webmd.com/depression](http://www.webmd.com/depression)' can be every bit as revealing as the content of an email message."

"Under the Bush administration, officials in security agencies had disclosed to reporters the large-scale collection of call records data by the NSA," Greenwald wrote, "but this is the first time significant and top-secret documents have revealed the continuation of the practice on

a massive scale under President Obama.” He added, “The unlimited nature of the records being handed over to the NSA is extremely unusual. FISA court orders typically direct the production of records pertaining to a specific named target who is suspected of being an agent of a terrorist group or foreign state, or a finite set of individually named targets.”

Ron Wyden and Mark Udall, members of the Senate select committee on intelligence, have been reviewing secret intelligence collections operations for a long time. “We believe most Americans would be stunned to learn the details of how these secret court opinions have interpreted Section 215 of the Patriot Act,” they wrote in a letter to Attorney General Eric Holder last year.

“After years of review,” Wyden and Udall wrote after Snowden’s revelations, “we believe statements that this very broad Patriot Act collection has been ‘a critical tool in protecting the nation’ do not appear to hold up under close scrutiny. We remain unconvinced that the secret Patriot Act collection has actually provided any uniquely valuable intelligence.” They added, “As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.”

According to Wyden and Udall, “When Americans call their friends and family, whom they call, when they call, and where they call from is private information. We believe the large-scale collection of this information by the government has a very significant impact on Americans’ privacy, whether senior government officials recognize that fact or not.”

In addition, Greenwald, and the Washington Post, reported on the existence of PRISM, the NSA’s Internet surveillance system that collects data from Google, Yahoo, Microsoft, Facebook, PalTalk, AOL, Skype, YouTube and Apple. Established pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA) and the 2008 FISA Amendments Act, PRISM allows national security officials to collect material including search history, the content of emails, file transfers and live chats, if targeted at foreigners “reasonably believed” to be abroad, even if the surveillance takes place on US soil. The law forbids intentionally targeting data collection at American citizens or anyone in the United States. But, according to Greenwald,

“The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.”

According to materials obtained by the Post, “NSA reporting increasingly relies on PRISM” as its primary source of raw material, and accounts for one in seven intelligence reports.

After the surveillance became public, a senior intelligence official who spoke anonymously to the New York Times claimed that PRISM thwarted a 2009 plot by Najibullah Zazi to bomb the New York City subway system. But public legal documents reveal that “old-fashioned police work, not data mining, was the tool that led counterterrorism agents to arrest Zazi,” according to Ben Smith at BuzzFeed.

Snowden revealed the secret information because, he said, “What they’re doing” poses “an existential threat to democracy.” He leaked the documents at great risk to himself. “I’m willing to sacrifice [his home and family] because I can’t in good conscience allow the US

government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building."

Snowden said,

"Everyone, everywhere now understands how bad things have gotten - and they're talking about it. They have the power to decide for themselves whether they are willing to sacrifice their privacy to the surveillance state."

The contrast between liberty and security is not a new one. Benjamin Franklin warned, "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor security." Throughout our history, we have grappled with this apparent tension. Unfortunately, all too often, we have lost our liberties - with no tangible benefit.

Senator Dianne Feinstein, chairwoman of the Senate Intelligence Committee, defended the massive intelligence-gathering program, while admitting she did not know how the collected data was being used. The New York Times called her defense "absurd." Greenwald tweeted, "The reason there are leakers is precisely because the govt is filled with people like Dianne Feinstein who do horrendous things in secret."

When Obama ran for president in 2008, he promised change - change from the policies of the Bush administration. The only change he has made in the Bush surveillance policy is to increase it to dragnet-like proportions.

Both Congress - by dutifully rubber-stamping the executive's requests for almost unlimited snooping powers - and the courts - by affirming those policies - have acquiesced in the unprecedented surveillance of us all. It thus remains for We the People to pressure the government to heed Benjamin Franklin's chilling admonition. As Snowden said, "It's important to send a message to government that people will not be intimidated." If we don't, we will live in nothing less than a police state.

*Marjorie Cohn is a professor at Thomas Jefferson School of Law, former president of the National Lawyers Guild and deputy secretary general of the International Association of Democratic Lawyers. Her most recent book is [The United States and Torture: Interrogation, Incarceration, and Abuse](#). She is working on a book about drones and targeted killing. [Originally published by Truthout](#). Reprinted with permission.*

The original source of this article is [Truthout](#)  
Copyright © [Prof. Marjorie Cohn](#), [Truthout](#), 2013

---

**[Comment on Global Research Articles on our Facebook page](#)**

**[Become a Member of Global Research](#)**

Articles by: [Prof. Marjorie Cohn](#)

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)

[www.globalresearch.ca](http://www.globalresearch.ca) contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)