Thank You, Edward Snowden

"The NSA has turned the internet into a giant surveillance platform."

By: Ronald Bailey - October 18, 2013

Last week the Cato Institute put on a terrific conference about unconstitutional domestic spying. The Cato conference took place after a summer of alarming revelations of just how deep and extensive the feds' secret surveillance of our everyday communications had become. The conference, held at the institute's downtown D.C. headquarters, brought some of the most knowledgeable Internet luminaries together with some of the fiercest fighters for Americans' Fourth Amendment rights.

Watchdog organizations such as the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) had sought for years to expose the extent and depth of federal surveillance, but their efforts were largely stymied by the very walls of secrecy they were trying to breach. In the 2006 case Hepting v. AT&T, for example, the EFF sued the giant telco for the privacy violations incurred by allowing the National Security Agency (NSA) to wiretap and data-mine all of the company's customers' communications. To forestall this case, Congress in 2008 passed the FISA Amendments Act, conferring retroactive immunity on the telephone companies and government agencies for engaging in warrantless wiretapping. Earlier this year, the U.S. Supreme Court rejected a challenge to the FISA Amendments Act by the ACLU and other groups, on the grounds that they had no standing to sue because they could not actually prove that the NSA was spying on them. This is Catch-22 logic: The ACLU needs to sue the NSA to get the evidence that the agency spied on it and its clients, but they can't sue because they have no evidence that the agency spied on them.

The walls of surveillance secrecy were finally cracked by the June revelations of whistleblower Edward Snowden. Snowden's files conclusively show that the federal government has been operating a vast spying program that violates the Fourth Amendment rights of tens of millions of ordinary Americans. To justify this surveillance, the government offers tortured legal interpretations of Section 702 of the Foreign Intelligence Surveillance Act and Section 215 of the PATRIOT Act.

Section 702 authorizes warrantless surveillance of the communications of foreigners outside of the United States. As Snowden's documents reveal, the NSA has interpreted Section 702 as a backdoor loophole allowing the agency to retain and comb through the call data and emails of Americans whose communications are "about" a terror suspect or have been "inadvertently" intercepted by the NSA's PRISM monitoring program. The even more egregious violations of our constitutional rights, Snowden revealed, occurred under Section 215 of the PATRIOT Act, which the NSA has used to justify the dragnet

collection and retention of the call metadata of essentially all Americans. (Metadata includes the numbers called and the location, date, time, and duration of each call.)

The first keynote at the Cato conference was delivered by Sen. Ron Wyden (D-Ore.), who cited the "revelations of June" numerous times. Several speakers used such circumlocutions during the conference, clearly as a way to avoid actually speaking the name of the man who finally broke the news that our government has been unconstitutionally spying on us for years. Despite his reticence with regard to Snowden, Wyden has been at the lonely forefront of the fight to rein in America's growing surveillance state. It was Wyden who asked Director of National Intelligence James Clapper in a March hearing whether the agency collected any sort of data on hundreds of millions of Americans. "No, sir," lied Clapper. "Not wittingly."

After Snowden's revelations proved that Clapper was a liar, Clapper attempted to justify himself in a June television interview by suggesting that "collect" doesn't mean the same thing to him that it means to ordinary Americans. "Collect," Clapper claimed, doesn't mean intercepting and storing data about telephone calls; the data are only "collected" when the agency goes searching through its vast databases looking for specific calls. At the Cato conference, New York Times national security reporter Charlie Savage pointed out that "Congress doesn't know that there is a secret lexicon at the NSA in which words mean something else at the NSA." He recommended that people might want to look up the Electronic Frontier Foundation's helpful NSA glossary, which shows how the agency reinterprets normal words in ways that ordinary people would say amount to "lies." Another speaker, Rep. Justin Amash (R-Mich.), said that Clapper should step down and be prosecuted for lying to Congress.

During his morning keynote, Wyden outlined the main provisions of a new bill he introduced with Sens. Mark Udall (D-Utah), Richard Blumenthal (D-Conn.), and Rand Paul (R-Ky.) two weeks earlier. The bill would end the mass collection of American's communication data, close the backdoor search loophole under FISA Section 702, provide an advocate to argue against government abuses before the Foreign Intelligence Surveillance Court, and enable citizens to be heard in federal courts when they believe that the surveillance agencies have violated their Fourth Amendment right to privacy. In addition, telecommunications companies would be enabled to disclose more information about their cooperation with government surveillance activities.

Wyden warned that the agency heads and their enablers in the Congress, such as Senate Intelligence Committee Chair Dianne Feinstein (D-Calif.), would be striking back against proposals for increased transparency. "Their objective is to fog up the surveillance debate," he explained, "and convince Congress and the public that the real problem is not unconstitutional surveillance, the real problem is sensationalistic reporting." Wyden is encouraged, however, by the broader reaction to the "revelations of June." Referring to the Amash amendment, a July measure that sought to cut funding to the NSA's bulk collection of Americans' phone records, Wyden said, "If you'd told me that you could get 200 votes on the floor of the House of Representative, I would have said you're dreaming." The amendment failed, but the vote was surprisingly close.

Of course, that vote was only possible because of Snowden's disclosures. Yet in July, when Wyden was asked whether Snowden is a hero or a villain, he replied that "when there is an individual who's been charged criminally and he has been charged with espionage, I don't get into commenting beyond that." Wyden should comment, and his comment should be: "Thank you, Edward Snowden."

Next up at the conference was a panel of national security reporters moderated by Cato's Julian Sanchez. The panelists were Bart Gellman of the Washington Post, Spencer Ackerman of The Guardian, Siobhan Gorman of The Wall Street Journal, and Charlie Savage of The New York Times. Gellman was the first speaker to say the word "Snowden," noting that the whistleblower's greatest fear was that the risks he took would be all for nothing; that there would be no debate over the extent and intrusiveness of domestic surveillance. In fact, Gellman declared, "Snowden succeeded beyond his wildest dreams."

Gellman also said that Clapper wasn't the only administration official to lie to Congress. NSA chief Keith Alexander wasn't telling the truth when he claimed a year ago that his agency does "not hold data on U.S. citizens" at its gigantic new data facility in Bluffdale, Utah. And the Justice Department had certainly been misleading, even if it didn't technically lie, when it said the Section 215 authorities had been used only 20 to 30 times to collect data. Yes, but those 20 to 30 times allowed the NSA to collect trillions of records.

Gorman added that the Snowden revelations had "shaken the trees" and prompted other reporting that has forced other government disclosures about various domestic spying efforts. For example, the NSA has tapped the Internet backbone through secret agreements with nine major (but unnamed) U.S. telecommunications companies. This has given the agency the capacity to monitor 75 percent of all U.S. Internet communications. Once it was revealed that the big telecommunications companies were cooperating with the NSA spying program, Gellman noted, they started agitating to be allowed to disclose more about what they are being asked and ordered to do.

The luncheon keynote was delivered by Rep. Amash, who described how spy agencies try to limit congressional access to information about their activities, making meaningful oversight all but impossible. Agencies speak in generalities and then engage in a game of 20 questions with legislators who seek deeper knowledge. They might, for example, answer a query with "No, our agency doesn't do that" without mentioning that another agency does.

Amash described one occasion in which he was seeking to review a particular document and the agency promised to arrange for members of Congress to do so. The agency did not send a message that the document was available for scrutiny by emailing members' offices directly; instead it sent the notification through the more general and less read Dear Colleague email system. Even then, the document was available for review only between 9 a.m. and noon in a briefing room on the day just before Congress was scheduled to leave for vacation. Members who reviewed the document also had to sign a nondisclosure agreement saying that they would not discuss it with other members who had not seen it.

After lunch, the conference featured a panel of legal experts, many of whom have tangled in court with the NSA and the Justice Department. Georgetown law professor Laura Donohue argued that the Foreign

Intelligence Surveillance Court (FISC) was solely created to supervise spying on foreign powers and their agents. Under statute, the FISC is supposed to review and grant orders under Section 215 only when agencies supply "a statement of fact showing that there are reasonable grounds to believe that tangible things sought are relevant to an authorized investigation."

Donohue argues that the FISC and the NSA have now interpreted "relevant" to include all data on all telephone calls, and possibly other records, such as data on all emails, financial records, medical records, and so forth. As such, Section 215 orders function as general warrants allowing officials to rifle through the records of any American without the need to show probable cause as delimited by the Fourth Amendment.

The ACLU's Jameel Jaffer agreed that the NSA's dragnet collection of phone records violates the relevance standard of Section 215. He also argued that it violated Americans' reasonable expectations of privacy under the Fourth Amendment and, less obviously, our right of free association under the First Amendment. If people think they are watched by government agents, he explained, they may curtail innocuous contacts with others out of fear that government functionaries will misinterpret or abuse information about their relationships. David Lieber, privacy counsel for Google, struck another First Amendment note, expressing frustration over the government's prior restraint of speech when it forbade his company (and others) from disclosing even summary statistics on how much information on its customers the feds were requiring it to turn over.

Paul Rosenzweig, a former deputy assistant for policy at the Department of Homeland Security, is much more sanguine about NSA domestic surveillance. He offered a very nice demonstration, produced by journalist Kieran Healy based on David Hackett Fischer's biography of Paul Revere, showing how metadata on various club memberships would have identified Paul Revere to the British authorities as the center of terrorist network in late-18th-century Boston. That may sound alarming to you, but to Rosenzweig the NSA's use of such relational data-mining is "relevant" to an investigation.

The second afternoon panel focused on techniques to protect data from federal surveillance. First, the good news: Jim Burrows of Silent Circle, a new company offering various encryption services, observed that TOR, the free open source software that protects users' anonymity, generally stands up to NSA snooping. Less happily, David Dahl of SpiderOak, a company that offers encrypted file backup, decried the recent revelations that the NSA had succeeded in introducing subtle vulnerabilities by influencing the development of encryption standards. Matt Blaze, an Internet security guru at the University of Pennsylvania, observed that maintaining vulnerabilities in computer code doesn't just make it easier for the NSA to spy; it makes it easier for the Chinese, Russians, and Iranians to spy, and for Internet criminals to steal data and cause other havoc.

Burrows discussed the case of Lavabit, an encrypted email service apparently used by Snowden. The NSA ordered Ladar Levison, the owner of the service, to hand over data that would enable the agency to spy on his 350,000 customers. Levison instead shut down the service, saying that he refused "to become complicit in crimes against the American people." Burrows noted that Silent Circle was also an offering encrypted email service. Within 10 hours of learning what had happened to Lavabit, Silent Circle shut

down and purged its own service without notice to subscribers. Burrows noted that had Silent Circle informed its customers in advance the shutdown might have become illegal. “We knew for sure that someday some law enforcement agency would order us to give them a backdoor,” said Burrows.

Burrows noted that there is no email that is currently secure against metadata collection, although users can securely encrypt the content of their messages. The ACLU’s Chris Soghoian added that the laws of physics make it impossible to shield the location data emitted by mobile phones. SpiderOak’s Dahl speculated that some peer-to-peer communications protocols with built-in cryptography might make secure email possible.

The final panel considered what reforms are necessary to rein in domestic surveillance. Cato Senior Fellow John Mueller demolished the claim that the NSA’s domestic spying has done much to protect Americans against terrorism. NSA chief Alexander claimed in June that mass telephone surveillance program had thwarted 54 terrorist plots. In October, Alexander admitted in a Senate hearing that the telephone dragnet’s effect was much more modest: It may have helped in one or maybe two cases.

“The Obama administration has doubled down on this program and doesn’t believe that it has done anything wrong,” despaired Michelle Richardson, legislative counsel for the ACLU. Center for Democracy and Technology senior counsel Kevin Bankston remarked that it is “insane” that Google’s privacy counselor David Lieber “had to dance around the question of receiving requests from the NSA.” People are free to say they haven’t received such requests, but they’re not allowed to tell anyone when they have.

“The NSA has turned the Internet into a giant surveillance platform,” declared renowned tech guru and Harvard Berkman Center fellow Bruce Schneier. Metadata collection that tells spies where a person went, who he spoke to, what he bought, and what he saw equals surveillance. “When the president says, ‘It’s just metadata,’” he means, “Don’t worry, you’re all under surveillance all of the time.” Schneier argued that we need to make the Internet secure against all attackers. “A secure Internet is in everyone’s interests,” said Schneier. “We are all better off if no one can do this kind of bulk surveillance. Fundamentally, security is more important than surveillance.” The panel agreed that it is critical to pass legislation preventing the government from mandating that companies build spy-friendly insecurities into their systems.

The final keynote speaker, Rep. James Sensenbrenner (R–Wisc.), outlined the contours of his Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection, and Online Monitoring (USA FREEDOM) Act. His bill would limit the collection of phone records to known terrorist suspects, force the Foreign Intelligence Surveillance Courts to disclose surveillance policies, establish a constitutional privacy advocate in that court’s proceedings, and permit companies to disclose NSA information requests.

At the end of conference, the one person whose efforts made it possible to for new Congressional reform efforts aimed at reining in the surveillance state went largely unacknowledged. And so, again: Thank you, Edward Snowden.