**“NSA must prove value of phone program” by The Editorial Board, Usatoday.com**

Since fugitive leaker Edward Snowden burst on the scene in June, Americans have learned a lot about all the ways in which their government is watching them. Among the most disturbing:

* For seven years, the National Security Agency (NSA) has been collecting detailed phone data on hundreds of millions of Americans not suspected of anything.
* The NSA is harvesting millions of e-mail and instant messaging contact lists. Though the program is targeted at foreigners, it sweeps in many ordinary Americans, [*The Washington Post* reported last week](http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html).
* The NSA is building a [1-million-square-foot fortress in Utah](http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/) to hold a massive collection of data. NSA Director Keith Alexander is bent on sweeping in the whole "haystack to find the needle," while other top intelligence officials talk of needing "all the dots" in order to connect them.

The problem is, they're not really talking about hay or dots. They're talking about collecting massive amounts of data on just about everyone in the United States so the government will have it around in case it's needed.

Until Snowden's revelations made headlines, most lawmakers knew little about these collections. Now Congress is considering whether to curtail or kill the phone records program — the most expansive of the initiatives that have been exposed and a test of where to draw the line between what the government wants and what it actually needs.

In that debate, the burden should be on the NSA to prove that the program's benefits outweigh its costs, which Alexander has struggled to do.

Initially in June, he testified that the phone database, along with a less intrusive e-mail program targeting foreign suspects, had helped disrupt "potential terrorist events over 50 times since 9/11."

By July, under skeptical questioning by Senate Judiciary Chairman Patrick Leahy, D-Vt., Alexander's deputy said the phone data "[made a contribution](http://articles.washingtonpost.com/2013-07-31/world/40905899_1_phone-records-nsa-xkeyscore/2)" in just 12 cases. And at a symposium in Aspen, when asked how often phone data were the "tip-off" to a plot, [Alexander replied](http://www.aspeninstitute.org/events/2013/07/17/2013-aspen-security-forum/transcript-clear-present-danger-cyber-crime-cyber): "I don't have the numbers off the top of my head to break it out like that."

Now supporters of the program have fallen back on what-ifs about 9/11. If intelligence agencies had phone metadata before 9/11, they argue, it would have revealed one of the terrorists who was in the U.S. well before the attack. Talk about rewriting history. The tragic flaw before 9/11 was not lack of data but failure to share what agencies already knew.

Even if today's officials are well-intentioned, which they seem to be, the potential that such a resource will be abused is significant, particularly if access to it is one day expanded to the many agencies that would find such tracking useful. The abuses by the FBI under J. Edgar Hoover are instructive, as are the political manipulations of Richard Nixon.

A number of lawmakers — Democrats and Republicans, left and right — have criticized this program as too intrusive. Among them are Leahy and conservative Rep. James Sensenbrenner, R-Wis., a key architect of the 2001 law that carved out broad new powers to prevent terrorism. They would end the program. Others would add new protections, such as greater judicial oversight.

Choosing between privacy rights and security from terrorism is difficult. But before Americans are forced to make that choice, the government ought to demonstrate that this intrusive program has extraordinary value. So far, the administration hasn't even come close.

Works Cited:

The Editorial Board. "NSA Must Prove Value of Program”." *USAToday.com*. N.p., 20 Oct. 2013. Web. 16 Oct. 2014.

**Sen. Dianne Feinstein: “Continue NSA call-records program”**

By Dianne Feinstein, usatoday.com

October 20, 2013

The NSA call-records program is legal and subject to extensive congressional and judicial oversight. Above all, the program has been effective in helping to prevent terrorist plots against the U.S. and our allies. Congress should adopt reforms to improve transparency and privacy protections, but I believe the program should continue.

The call-records program is not surveillance. It does not collect the content of any communication, nor do the records include names or locations. The NSA only collects the type of information found on a telephone bill: phone numbers of calls placed and received, the time of the calls and duration. The Supreme Court has held this "metadata" is not protected under the Fourth Amendment.

This program helps "connect the dots" — the main failure of our intelligence before 9/11. Former FBI director Robert Mueller and Director of National Intelligence James Clapper testified that if this program existed before 9/11, it likely would have identified the presence inside the U.S. of hijacker Khalid al-Mihdhar.

The NSA uses these records to identify connections between known and suspected terrorists (as well as terror conspirators and supporters). The overwhelming majority of records are never reviewed before being destroyed, but it is necessary for the NSA to obtain "the haystack" of records in order to find the terrorist "needle."

Only a strictly limited number of NSA analysts (among the thousands of professionals at the agency) may search the phone records database and only after articulating a specific reason that must be approved by a senior official. Those decisions are reviewed regularly by the Justice Department, Congress and the Foreign Intelligence Surveillance Act (FISA) Court, which imposes strict privacy protections.

To be effective, the NSA must be able to conduct these queries quickly, without regard to which phone carrier a terrorist or conspirator uses. And the records must be available for a few years — longer than phone companies need them for billing purposes.

Since its inception, this program has played a role in stopping roughly a dozen terror plots and identifying terrorism supporters in the U.S. Given the threats we face from al-Qaeda and others, we need all legal tools at our disposal.

The Senate Intelligence Committee will soon consider legislation to add public reporting requirements and more court review, and to codify existing procedures into law. I hope this will restore public confidence to a program that continues to protect the homeland from terrorism.

*Sen. Dianne Feinstein, D-Calif., is chairman of the Senate Intelligence Committee.*

Works Cited:

Feinstein, Dianne. "Sen. Dianne Feinstein: “Continue NSA Call-records Program”." USAToday.com. N.p., 20 Oct. 2013. Web. 16 Oct. 2014.

Google's Eric Schmidt calls NSA surveillance 'outrageous'

By Adi Robertson, Theverge.com

November 4, 2013

After leaked documents apparently revealed that the NSA has been [collecting Google and Yahoo user information](http://www.theverge.com/2013/10/30/5046958/nsa-secretly-taps-into-google-yahoo-networks-to-collect-information) as it travels between servers, Google executive Eric Schmidt says the American surveillance program is violating everyone's privacy for the sake of catching a few suspicious messages. "It's really outrageous that the National Security Agency was looking between the Google data centers, if that's true," he told *The Wall Street Journal's*Deborah Kan*.* "The steps that the organization was willing to do without good judgment to pursue its mission and potentially violate people's privacy, it's not okay. It's just not okay."

Schmidt argued that the risk of terrorism doesn't justify secret mass surveillance. "Let's start with appropriate oversight and appropriate transparency," he said. "There clearly are cases where evil people exist, but you don't have to violate the privacy of every single citizen in America in order to find them!" He referenced a [statement by NSA head Keith Alexander](http://www.theverge.com/2013/6/18/4441774/over-50-terrorist-plots-stopped-NSA-surveillance), who said in June that fewer than 300 numbers were used to query the agency's massive phone record database: "The NSA allegedly collected the phone records of 320 million people in order to identify roughly 300 people who might be a risk. It's just bad public policy."

"IT'S JUST BAD PUBLIC POLICY."

Google has previously assailed the secrecy of decisions made under the Foreign Intelligence Surveillance Act, which forbids companies to disclose how much information they've given to the government or how many requests they've received. A pending lawsuit argues that revealing some information would not threaten the US intelligence community, and that national security gag orders are a First Amendment violation that damages Google's public image by not letting it set the record straight. The company is also one of several [lobbying Congress to reform the NSA](http://www.theverge.com/2013/10/31/5053438/apple-microsoft-google-and-others-urge-congress-to-enact-nsa-reforms) by introducing more limits and transparency, and it's steadily denied providing anything more than the bare minimum of information to intelligence agencies.

In his interview, Schmidt also discussed Google's other policy decisions, like its withdrawal from mainland China in 2010. "China's censorship regime has gotten significantly worse since we left," he said, "so something would have to change before we come back." While Google has left China, Schmidt himself has been visiting countries like Burma and North Korea, attempting to chip away at restrictions that keep citizens offline and isolated. His next move, he told Kan, will be Cuba — whose locked-down internet traffic was carried across slow satellite links for years before an underwater cable was finally turned on [earlier this year](http://www.theverge.com/2013/1/24/3912274/cuba-confirms-underwater-data-cable-turned-on).

Works Cited:

Robertson, Art. "Google’s Eric Schmidt calls NSA Surveillance ‘Outrageous’." Web log post. Theverge.com. N.p., 4 November 2013. Web. 16 Oct. 2014.

**5 Reasons Why The NSA's Massive Surveillance Program Is No Big Deal (And 2 Reasons It Is)**

By David Francis, *Thefiscaltimes.com*

July 11, 2013

Edward Snowden, the 29-year old Booz Allen Hamilton contractor who leaked secret NSA documents, has disappeared and according to reports, has [checked out](http://www.washingtonpost.com/world/asia_pacific/hong-kong-hotel-says-edward-snowden-was-there-but-checked-out-monday/2013/06/10/44baa0fa-d1af-11e2-a73e-826d299ff459_story.html) of his Hong Kong hotel.

He was advised not stay in Hong Kong because there is a strong extradition treaty between China and the United States. Snowden suggested over the weekend that he would apply for asylum in Iceland.

His disappearance is the latest in a series of twists in the controversy over the PRISM program and public surveillance in the United States, including the deep access the federal government has to personal information.

Civil libertarians have cried foul, saying the data mining violated personal privacy and the 4th Amendment’s protection against unlawful search. Lawmakers on both sides of the isle fired back, claiming that the surveillance programs were necessary to prevent terrorism and that revealing information about them gives an advantage to U.S. enemies.

“Right now, we know that there are [active threats against the United States](http://thehill.com/blogs/floor-action/house/304409-cantor-congress-will-launch-very-serious-investigation-into-snowden)," Rep. Eric Cantor (R-Va.) said Sunday morning. "We have terrorist threats that continue. There are possible security incidences that continue. And that's just the world that we live in.”

Cantor said the House of Representatives would investigate Snowden’s actions. White House spokesperson Tim Carney declined to comment on Snowden Monday. He said President Obama "would welcome" a conversation about surveillance but not about the leaks that caused it.

There are still lingering questions about whether these revelations actually give terrorists and other countries a leg up against the United States. Here are five reasons that PRISM is no big deal, as well as two reasons why Americans need to be worried about what the government and its 5 million security-cleared workers could do.

1. Online surveillance has been effective and is an important tool in the fight against terrorism. Lawmakers have said that data mining stopped attacks in the United States and overseas. The programs also provide U.S. authorities with leads on potential and existing terrorists. One NSA official told the Washington Post that PRISM provided a “[field of dots](http://www.washingtonpost.com/opinions/marc-thiessen-leaks-not-the-nsa-programs-deserve-condemnation/2013/06/10/e91d09ac-d1c9-11e2-a73e-826d299ff459_story.html?hpid=z4)” which allowed authorities to connect the relevant ones.

But the best justification for the program has been what has not occurred. Since 9/11, there has only been one major terror attack on U.S. soil.

2. We’ve been under surveillance for more than a decade. The government has been monitoring online and telephone activity for more than a decade. During the Bush years, NSA was able to [monitor phone calls without a warrant](http://www.thefiscaltimes.com/Articles/2013/06/09/After-Years-Americans-Are-Resigned-to-Surveillance.aspx#page1).

President Obama said he has put strict protocols in place that require judicial review and a warrant for all PRISM targets. He and other officials also said the government is not listening to your conversations or reading your email. It’s simply identifying phone numbers that could be connected to terrorists.

3. Private businesses are collecting data too. The government isn’t the only one in the data collection business. Private businesses are also are mining data.

4. Any terrorist who doesn’t think they’re under constant surveillance is an amateur. Effective terrorists aren’t stupid; the 2001 terrorist attack proved that. The truly dangerous ones know they are under constant surveillance and take steps to avoid detection. Any would-be jihadist who uses their mobile phone to explicitly make plans to destroy America is probably not a danger (and is also probably headed to a secret prison).

5. We’re all complicit in this. Americans love to share data. We post photos and videos on social media without a second thought. Rarely do we think about what they’re letting the world know.

For instance, I can outright determine or logically deduce the following things about the most active people in my Facebook feed: where they live; where they work; roughly how much money they make; how many children they have; where their children go to school; what time they drop off and pick up these kids at school; where they vacation; where they spend social time; what and when they eat; what family and interpersonal issues they’re having; their politics; where they were educated; their television and reading habits; what music they listen to; and when they and the other members of their family were born.

All of this - and much, much more - can be determined with just a brief visit to Facebook. Why are people worried about the government invading their privacy when they’ve been volunteering private information online for years?

This is not to say that PRISM doesn’t raise concerns. Here are two reasons we should all be worrying about the surveillance capabilities the government now has.

1. Where does it stop? Snowden said the government has the ability to listen to phone calls and read emails of all Americans. All that was collected was data. There is no indication that the government has used data improperly. Yet.

“We have no assurance that the harvested information will not be misappropriated, like we see with Patriot Act laws being used against drug offenders, and government officials using the justification of 'national security' to monitor anti-war demonstrators, as well as the activity of Code Pink and Ron Paul supporters, and opponents of natural gas drilling," said Malou Innocent, a foreign policy analysts at the libertarian Cato Institute.

2. How many 29-year old high school dropouts have access to top-secret information? Snowden received his GED and did not complete college, yet he had access to some of the most classified information in the world. And he showed little hesitancy is leaking this information to the press, a betrayal he said he made because in the best interest of America.

According to a report in the [Wall Street Journal](http://www.theatlanticwire.com/national/2013/06/contract-security-clearance-charts/66059/), nearly five million people have security clearance. Some 1.4 million of those people have access to the country’s most sensitive information. Of those, one third are contractors.

Education levels of these workers are unknown, but it’s safe to say that most of them probably graduated from high school, if not college and graduate school as well. Still, Snowden showed that all it takes is one disgruntled employee to spill the country’s darkest secrets. There are a lot of potential leakers in a workforce of 1.4 million.

Works Cited:

Frances, David. "5 Reasons Why The NSA's Massive Surveillance Program Is No Big Deal (And 2 Reasons It Is)." Web log post. Thefiscaltimes.com. N.p., 11 July 2013. Web. 16 Oct. 2014